أكاديمية نايف العربية للعلوم الأمنية
كلية الدراسات العليا
قسم العلوم الشرطية

وسائل التحقيق في جرائم نظم المعلومات

رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية

إعداد
النقيب/ سليمان مهجع العنزي

إشراف
د . رشيد مسفر أحمد الزهراني
رئيس قسم نظم المعلومات/ كلية علوم الحاسب والمعلومات
جامعة الملك سعود

الرياض ١٤٢٤هـ – ٢٠٠٣م

العلوم الشرطية

قيادة أمنية

√

وسائل التحقيق في جرائم نظم المعلومات.

سليمان مهجع العنزي
د . رشيد مسفر أحمد الزهراني

د . رشيد مسفر أحمد الزهرانـــي (مشرفاً ومقرراً)

د . عبد الله عبد العزيز الموســـى (عضـــــــوأ)

اللواء د . محمد فاروق عبد الحميد (عضـــــــوأ)

٢٥ ٣ ٢٤ ٢٦ ٥ ٠٣

يتطلب التحقيق في جرائم نظم المعلومات معرفة أساليب وأدوات ومنافذ ارتكابها، وإيضاح الوسائل المساعدة في توفير الأدلة المثبتة على وقوعها وتحديد شخصية مرتكبها. ولذا يمكن صياغتها عبر السؤال التالي: ما الوسائل المساعدة بالتحقيق في جرائم نظم المعلومات، وكيف تستغل بصورة فاعلة للوصول مجرمي نظم المعلومات؟

ستكون هذه الدراسة مرجعاً للعاملين في الأجهزة الأمنية في مجال معرفة وسائل التحقيق في جرائم نظم المعلومات وكيفية مساهمتها في تسهيل أعمال التحقيق. كما يمكن أن تقدم للعاملين في مجالات نظم المعلومات إطاراً لكيفية الانسجام مع المتطلبات الأمنية اللازمة لأعمال التحقيق. وقد تفيد الجهات المتضررة من هذه الجرائم في وضع سياسة أمنية شاملة لحماية نظم معلوماتها. كما تسهل وضع سياسة تدريبية للعاملين في أمن المعلومات ليتمكنوا من التحقيق بتلك الجرائم، ليكونوا قادرين على مواجهة تحديات التطور الهائل في أساليب ارتكاب هذه الجرائم.

سعت هذه الدراسة إلى تحقيق الأهداف التالية: وضع إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات. وتحديد أنماط جرائم نظم المعلومات، ومدى حدوثها بالمؤسسات، وأضرارها، ودوافعها. حصر الأساليب المستخدمة في ارتكاب جرائم نظم المعلومات ومنافذها. وحصر الأدوات المستخدمة من قبل مجرمي نظم المعلومات وكيف يمكن لمجرمي نظم المعلومات بالمملكة أن يحصلوا عليها. والكشف عن وسائل التحقيق في جرائم نظم المعلومات. وبيان العوائق التي تحول دون استخدام تلك الوسائل. وتحديد أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات.

ما العناصر المكونة للسياسة الأمنية الشاملة لحماية نظم المعلومات وما مدى وضوح تلك العناصر بالمؤسسات؟ وما الإجراءات الفنية والإدارية لتحقيق أمن نظم المعلومات وما مدى إتباعها من قبل المؤسسات؟، وما هي أنماط جرائم نظم المعلومات، وما مدى حدوثها بالمؤسسات، وأضرارها، ودوافعها؟، وما الأساليب المستخدمة في ارتكاب جرائم نظم المعلومات، ومنافذها؟، وما الأدوات المستخدمة من قبل مجرمي نظم المعلومات، وكيف يمكن أن يحصلوا عليها بالمملكة. وما وسائل التحقيق في جرائم نظم المعلومات، والعوائق التي تحول دون استخدام تلك الوسائل؟، وما أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات؟.

استخدم الباحث المنهج الوصفي من خلال أسلوب المسح الاجتماعي، كما استخدم استبانة مكونة من (١٩٤) فقرة، وذلك لجمع البيانات من أفراد عينة الدراسة والبالغ عددهم (١٤١) فرداً، منهم (٣٦) محققاً من شرطة الرياض والشؤون الفنية بوزارة الداخلية، و(٦٨) عاملاً بمجال نظم المعلومات في القطاع العام والخاص في مدن كل من الرياض، وجدة، والدمام، و(٣٧) متخصصاً في المؤسسات الموفرة لتقنيات أمن المعلومات في مدينة الرياض.

توصلت الدراسة إلى عدد من النتائج من أهمها؛ أن هناك برامج حماية تساعد بما نسبته (٩٤,٢٪) في تحديد نوع الجريمة، وما نسبته (٩٥,١٪) في تحديد توقيت ارتكابها وما نسبته (٧٥٪) في تحديد مصدرها، وما نسبته (٩٤,٢٪) في الإعلام بوجودها، كما أنه بالإمكان الاعتماد على عنوان (IP) (٩٤,٢٪)، وبرامج الحماية (٩١,٤٪)، وبرامج تتبع المخترقين (٧٤,٩٪)، وبرامج تتبع مصدر الرسائل الإلكترونية (٥٩,٦٪)، ووسائل أمن البيانات (٨٨,٥٪)، بتحديد شخصية مرتكب جريمة نظم المعلومات في المؤسسات. كما أن هناك أدوات مهمة تساعد بضبط الجريمة، وهي؛ سجل الصلاحيات للمستخدمين (٤,٩٤)، والتقارير التي تنتجها نظم أمن البيانات (٤,٨٦)، وبرامج النسخ الاحتياطي والتسجيل Logging (٤,٧٦)، وبرامج كشف الفيروسات (٤,٧٤)، وأدوات المراجعة Auditing (٤,٦٩)، وتقارير الجدران النارية (٤,٥٣)، وأدوات مراقبة المستخدمين للشبكة (٤,٥٢)، وبرامج تتبع المخترقين (٤,١١)، ومراجعة قاعدة البيانات (٤,٠٧)، وبرامج تتبع مصدر الرسائل (٤,٠٦). كما أن هناك أدوات تساعد بالتحقيق وهي؛ أداة فك التشفير (٣,٩٥)، وبرامج كسر كلمة المرور (٣,٩٣)، وأدوات استرجاع المعلومات من الأقراص التالفة (٣,٩٢)، وبرامج مقارنة النسخ (٣,٧٨)، وبرامج تشغيل الحاسب (٣,٢٩).

إهـــــداء

بكل احترام وتقدير صادق، وإخلاص، وولاء

لسيدي صاحب السمو الملكي

الأمـير/ خالد بن سلطان بن عـبـد العزيز آلـ سـعـود

مساعد وزير الدفاع والطيران والمفتش العام للشؤون العسكرية/ حفظه الله

أهــدي هــذا الجهد العلمي الصغير، إلى سمـوه الكـريم، الكـبير روحـاً وعلماً ومعرفة بكل مختلف العلوم الإدارية منها، والعسكرية، والأمنية، وعلوم الفضاء والطيران، والعلوم الاجتماعية، والنفسية، والقانونية، والاقتصادية، وجميع العلوم الطبيعية والتقنية.

شكر وعرفان

يشرفني أن أتقدم بخالص الشكر والعرفان لسعادة قائد قوة الصواريخ الاستراتيجية اللواء/ الركن/ زبن بن عيد العتيبي لتشجيع سعادته لمنسوبيه لاستكمال دراستهم العليا ودعمه الكبير واللامحدود لهم أثناء الدراسة ومتابعتهم وتسهيل جميع الصعاب التي تواجههم مما يرفع من تحصيلهم العلمي والروح المعنوية لديهم وينعكس على خدمة وطنهم.

كما أتقدم بخالص الشكر والعرفان لسعادة اللواء/ الركن/ عبد الرحمن بن إبراهيم الصغير مساعد قائد قوة الصواريخ الاستراتيجية على تشجيع سعادته لي ودعمه الكبير. كما أتقدم بوافر الشكر والعرفان وعظيم الامتنان لسعادة العميد/ الركن/ عواض بن ضاوي النفيعي مدير إدارة العمليات والتدريب بقوة الصواريخ الاستراتيجية, لتشجيعه، ودعمه، وتوجيهه، ومساعدته لي أثناء دراستي ومنذ بداية تفكيري بموضوع هذه الرسالة، وحرصه الشديد على إزالة جميع العقبات التي تواجهني، مما جعلني أشعر بسعادة عظيمة وأكن له كامل المحبة والتقدير.

كما أتقدم بخالص الشكر والعرفان لسعادة العميد/ الدكتور/ ناصر عبد العزيز المويشير قائد القاعدة (٥٢٢) لما بذله من جهود في سبيل تسهيل التحاقي بأكاديمية نايف العربية للعلوم الأمنية، وتشجيع سعادته لي ودعمه الكبير، كما أرفع خالص شكري وتقديري لسعادة الأستاذ الدكتور/ عبد العزيز بن صقر الغامدي رئيس أكاديمية نايف العربية للعلوم الأمنية, لما لمسناه منه قائداً ومطوراً في عمله, وأباً فاضلاً في معاملته. كما أتقدم بالشكر الكبير لمعالي الفريق الدكتور/عباس أبو شامة وزير الداخلية السوداني السابق رئيس قسم العلوم الشرطية على حسن التعامل والتوجيه المستمر.

كما أزجي خالص شكري وعظيم امتناني وتقديري لسعادة الدكتور/ رشيد بن مسفر الزهراني المشرف العلمي على هذه الرسالة ورئيس لجنة المناقشة, صاحب الفضل بعد الله في

تشجيعي ومساندتي في إنجاز هذه الرسالة بهذه الصورة، وتفضله بإعطائي وقتاً مفتوحاً لمقابلته في أي وقت أشاء، والعمل على توجيهي لإنجازها خارج الجامعة ووقت إجازاته الأسبوعية والرسمية. ولقد غمرني بلطفه، وحسن معاملته، وثقته التي منحني إياها. كما أشكر سعادة الدكتور عبد الله بن عبد العزيز الموسى عميد كلية الحاسب ونظم المعلومات جامعة الإمام محمد بن سعود الإسلامية وسعادة اللواء الدكتور/ محمد فاروق عبد الحميد عضو هيئة التدريس في أكاديمية نايف العربية للعلوم الأمنية على قبولهم مناقشة رسالتي.

وفي الختام أتوجه بالشكر والتقدير الكبيرين لسعادة العقيد/ المهندس/ الركن/ عبد العزيز بن عبيد الشمراني الذي سعى لترشيحي للدراسة وساهم أيضاً في تشجيعي وتوجيهي خلالها.

فهرس المحتويات

قائمة الأشكال

رقم الشكل **عنوان الشكل** **رقم الصفحة**

قائمة الملاحق

الفصل الأول/ نطاق المشكلة

١-١ المقدمة

تحتاج المؤسسات إلى تقنية تنظم تدفق معلوماتها وإداراتها، ومن هنا برزت الحاجة لنظم المعلومات التي ساهمت في أداء الأعمال بسرعة كبيرة ودقة عالية، وهذا الأسلوب الجديد بأداء الأعمال رافقه أسلوب جديد لارتكاب الجرائم يتطلب مواجهة من الأجهزة الأمنية بأسلوب جديد. ويتم ذلك بالمعرفة الجيدة بالنظام المعلوماتي وأسلوب حمايته وخصائص الجرائم المعلوماتية وأساليب وأدوات ارتكابها. ومن هنا جاءت فكرة هذه الدراسة والتي يبدأها الباحث في هذا الفصل بتمهيد، يستعرض فيه خلفية الدراسة، ومشكلتها، وأهميتها، وأهدافها، وتساؤلاتها وفرضيتها، والتعريفات الفنية والإجرائية.

١-٢ خلفية الدراسة

تعد المعلومات المقياس الذي تقاس به قوة الشعوب. فمن يملك المعلومات في هذا العصر مع القدرة على حمايتها يستطيع أن يسيطر، فالسيطرة لم تعد جيوشاً تغزو وأساطيل من الجيوش تجول فقط، بل هناك نماذج جديدة من السيطرة تتمثل بالسيطرة على المعلومات (داود، أ، ٢٠٠٠م: ٢٦). "لقد أدى التطور التقني والعلمي إلى وفرة المعلومات، وأصبح من الصعب التحكم في تدفق وانتقال المعلومات من مكان إلى آخر" (Spencer, ١٩٩٧: ١٦٣). "وأسفر هذا التقدم العلمي عن وسائل تقنية متطورة في معالجة البيانات والمعلومات بعد الحصول عليها من مصادرها المختلفة، لتحقيق الغرض النهائي من استخدامها والأهداف المنشودة من وراء العمل بها" (الرشيدي، ١٤٢٠هـ: ٣). ويعد الحاسب الآلي السلاح القوى في عصر المعلومات والأداة التي لا غنى عنها، لما له من القدرة الضخمة على تخزين المعلومات واسترجاعها عند الحاجة لها، والسرعة الهائلة التي تمكنه من التعامل

مع هذه المعلومات والربط بينها، واستخلاص المفيد منها، وما يتبع ذلك من قدرات متنامية على استنتاج ما تشير إليه هذه المعلومات من حقائق تكون في العادة خافية على متخذي القرار في غيبة تلك المعلومات ولا تظهر إلا في معالجة المعلومات المتوفرة وعرضها بالصورة الملائمة (داود، ب، ٢٠٠٠م: ١٤).

ظلت المؤسسات لفترة طويلة تعتمد على كمٍ كبيرٍ من النماذج والأشكال الورقية العديدة في المذكَّرات والاجتماعات واستمارات الموظفين إضافة إلى وثائقها الأخرى، وتستخدَمها في تناقل المعلومات في ما بينها، وقد عانت المؤسسات كثيراً من البطء في سير العمل وذلك لاعتمادها على هذه النظم الورقية المكلِفة (Itep, A, ٢٠٠٢). فإدارة المعلومات جزء لا يتجزأ من المؤسسة، وله أهميته نتيجة زيادة تعقد الأنشطة، والتطور الذي حدث في وسائل اتخاذ القرارات، وازدياد حجم المؤسسات، وازدياد استخدام التقنية بالمؤسسات، وكذلك الكم الهائل من البيانات الذي يحتاج إلى سرعة المعالجة (الحويطي، ١٤٢٢هـ: ٤٩). وكان أمراً ملحاً على المؤسسات التحول من التعامل التقليدي بالوثائق والأوراق، وحفظ خطوات الإنتاج بالاعتماد على العاملين فيها إلى التعامل بالنظم المعلوماتية، لتحسين الخدمات التي تقدمها تلك المؤسسات، ومنع التكرار في العمل، وتوفير الجهد، وتخفيض التكلفة، والسرعة في إنجاز العمل، وتطوير الإجراءات ورفع كفاءة أداء العاملين وزيادة كمية العمل المنجز والتعامل مع المعلومات بطريقة منظمة لمواجهة المتغيرات المستمرة واتخاذ القرارات السريعة والراشدة. "مما يتطلب بناء نظم معلومات ذات جودة عالية تلبي احتياجات المستفيدين بسرعة وفاعلية" (الشايع، ١٤٢٤هـ: ٢).

"كانت بداية نظم المعلومات عام ١٩٤٥م باستخدام الحاسب الآلي لإعداد قوائم الأجور والمرتبات" (السيد، بدون: ٣)، "إلا أن استخدام نظم المعلومات كمصطلح لم يبدأ إلا سنة ١٩٦٠م" (البكري، ١٩٨٥م: ٧١). وبدأت الحاجة تتزايد لتطوير نظم المعلومات لمواجه الحجم المتزايد لتشغيل البيانات. ومع تطور الأعمال ونمو التنظيمات الصناعية والخدمية أخذت نظم المعلومات في التطور

لسد تلك الحاجة، ولذا أصبحت نظم المعلومات اليوم نشاطاً عادياً لأي منشأة لأغراض التشغيل أو المراقبة أو دعم القرارات (الغامدي، ١٩٩٩م: ٤٩). وأسهمت نظم المعلومات في المؤسسات الضخمة بالتقليل من إجراءاتها اليدوية المعتمدة على الورق إلى اعتمادها على قواعد البيانات في تنظيم بياناتها، وشكّل ظهور الشبكات المحلية LAN والواسعة WAN والأنترانت Intranet والاكسترانت Extranet والإنترنت Internet حلولاً مناسبة لإيجاد شبكات اقتصادية وفعالة تسهل وتنظم تبادل المعلومات بين المؤسسات (Itep, A, ٢٠٠٢).

"تبين النتائج التي توصلت إليها إحدى المؤسسات الاستشارية (برايس واتر هاوس) حول أهمية نظم المعلومات للمؤسسات الإدارية بأنه إذا فقدت بعض المؤسسات نظم معلوماتها لمدة تزيد عن ثلاثة أيام متتالية، فإن نسبة احتمال إفلاسها تصل إلى (٦٠٪)، وإذا استمر فقدان الشركة لنظم معلوماتها لمدة شهر فإن نسبة خروجها من السوق وإفلاسها تقفز إلى (٩٠٪)" (التعزي، ١٤١٤هـ: ٢). أي انه كلما طالت مدة فقدانها لنظم معلوماتها زادت الخسائر المترتبة على ذلك.

ومع انتشار الإنترنت أصبحت لنظم المعلومات أهميتها في تنظيم التجارة الإلكترونية، فقد اتجهت كثير من المؤسسات العالمية إلى التسويق الإلكتروني للمنتجات وإيصال الخدمات وتلبية طلبات الشراء واستخدام البطاقات الائتمانية. "وعند تمرير رقم البطاقة عبر شبكة الإنترنت قد يمثل خطورة على صاحبها إذ يمكن لمخترق التقاطه مع المعلومات الأخرى المصاحبة لرقم البطاقة وإساءة استخدامها" (باتوباره، ١٤١٩هـ: ٢٠٦).

كما أن الاعتماد على نظم المعلومات في تزايد مستمر في القطاع المالي حيث يستخدم في تحويلات النقد وربط أسواق المال، مما وفر دافعاً قوياً للجريمة المؤسسة التي تملك المال والخبرات والتنظيم الذي يمكنها من ذلك (البشري، ١٤٢١هـ: ١٧٩). "وقد أفاد استطلاع اجري عام ١٩٩٤م في الولايات المتحدة الأمريكية لآراء مسئولي أمن الحاسبات الآلية أن هذه الجرائم تتزايد يوماً بعد يوم"

(المسند، والمهيني، ١٤٢١هـ: ٣٦٧). وبتعميم الحاسب الآلي في جميع نواحي الحياة وما حصل له من تطوير مستمر في مجالي التجهيزات والبرامج، ظهرت جرائم نظم المعلومات بصورة جديدة وبأعداد اكبر، وبخسائر أكثر.

بدأت أوائل عمليات الاختراق عام ١٩٨٥م و١٩٨٦م وقام بهذه العمليات الأمريكان والألمان، وتعد اشهر عملية اختراق عملية الطفل الأمريكي الذي يبلغ من العمر (١٤) سنه في عام ١٩٩٢م باختراقه لشبكة البنتاجون حيث سُمح له بإتمام عملية الاختراق لتحديد مكانه من خلال مزود الإنترنت بتتبعه عن طريق خطه الهاتفي وقد ضم هذا الطفل إلى فريق العمل في البنتاجون وأصبح أحد موظفيها الآن (العلي، ٢٠٠١م). ويوجد حوالي (٣٠) ألف موقع على الإنترنت، موجهة لأغراض الاختراق المختلفة، الأمر الذي أتاح البرامج المطوّرة لإطلاق الأنواع المختلفة من الفيروسات مجاناً، مما أدى إلى ارتفاع عدد الاختراقات حسب تقرير صدر عام ٢٠٠١م عن فريق طوارئ الحاسبComputer Emergency Response Team من (٢٠٠٠) اختراق سنة ١٩٩٧م إلى (٢١٠٠٠) اختراق سنة ٢٠٠٠م، وتشويه المواقع الذي قفز من (٥) حوادث سنة ١٩٩٥م إلى (٥٠٠٠) حادث في سنة ٢٠٠٠م (سليمان، ٢٠٠١م). ومن ضمن الجرائم التي تتعرض لها نظم المعلومات سرقة المعلومات للحصول على المال أو بهدف التجسس لأغراض عسكرية، مما قد يهدد الأمن القومي.

يستخدم مجرمو نظم المعلومات الفيروسات وديدان الإنترنت لإتلاف المعلومات، حيث أنها قادرة على التكاثر والانتشار بسرعة كبيرة (مجلة الأمن الإلكترونية، ٢٠٠٢م). ففيروس الحب مثلاً تسبب في خسائر تقدر بمليارات الدولارات إذ أتلف خمسة وأربعين مليون حاسب آلي في الرابع من مايو عام ٢٠٠٠م، ومن ضمن شبكات الحاسب الآلي التي تأثرت بهذا الفيروس تلك الخاصة بوزارة الدفاع الأمريكية، وكذلك الشبكة الخاصة بالبرلمان البريطاني (BBC, ٢٠٠١). كما يستخدم مجرمو نظم المعلومات برامج التجسس وإرسال المعلومات كبرامج Marker، وGroove Caligula، و Black

Orifice، وNet Bus، Sub Seven والتي تتميز بسهولة استخدامها وانتشار ملف التجسس الخاص بها في كثير من الأجهزة مما يجعل الاختراق بها سهلاً للغاية (Nanoart, ٢٠٠٢). وتسمح هذه البرامج لمجرمي نظم المعلومات في حال وصولها إلى أي جهاز حاسب الآلي من الأجهزة بالتحكم الكامل بالجهاز (مجلة الأمن الإلكترونية، ٢٠٠٢م).

ومن أشهر البرامج المستخدمة والقادرة على التحكم عن بعد والتي تستطيع تسخير هذه الأجهزة لتنفيذ الهجوم المنسق هو برنامج TFN (Tribe Flood Network)، كما يستخدم مجرمو نظم المعلومات برامج جديدة من أحصنة طروادة حيث أنها تدمج بين عدة خصائص، كأن يكون لها خاصية التكاثر مثل الفيروسات وعدم حاجتها لبرنامج محتضن تماماً مثل ديدان الإنترنت، ولديها القدرة على التعامل مع الملفات الصادرة أو الواردة من نوع FTP وHTTP وهي قادرة على تخطي وخداع الجدار الناري، وبالتالي جمع المعلومات من كلمات مرور وأسماء مستخدمين وأرقام بطاقات الائتمان، وكذلك تدمير بعض الملفات وتعديل مهامها (مجلة الأمن الإلكترونية، ٢٠٠٢م). ومازالت وسائل مجرمي نظم المعلومات في تزايد وانتشار سريع في ظل ضعف الاحتياطات الأمنية لمنع ارتكابهم لهذه الجرائم مما ساهم في تفاقم هذه المشكلة.

وإذا كان تبليغ الجهات الرسمية بوقوع جريمة عادية من قبل شخص عادي أو رجل أمن ممكناً، لوضوح عناصرها وتصنيفها القانوني، سواء وقعت في حقه أو حق غيره، بأن يقدم شهادته حولها بما رأى أو سمع، فإن العاملين بالأجهزة الأمنية يواجهون صعوبة في فهم الأركان والعناصر المكونة للجريمة المعلوماتية، وطرق ارتكابها والمراحل التي مرت بها ونتائجها المعقدة (البشري، ١٤٢١هـ). "وهذا ما جعل معتادي جرائم الحاسب الآلي Hackers يطلقون على أنفسهم صفة النخبة Elites بحجة انهم الأكثر معرفة بأسرار الحاسب الآلي ولغاتها المتميزة، بينما تطلق على رجال إنفاذ القوانين صفة الضعفاء Lamers" (البشري، ١٤٢١هـ: ٣٦٦).

ويختلف مسرح الجريمة المعلوماتية عن مسرح الجريمة التقليدية بصعوبة إثباتها وإظهار الأدلة لعدم وجود دليل مرئي، واحتياط الجاني بإجراءات احترازية فنية، أو بإزالة الدليل. ويتطلب كشف الأدلة تدريباً جيداً ومهارات خاصة وفهماً عميقاً لوسائل التقنية. ولقد أوضحت توصيات المؤتمر الدولي الثاني للاتجاهات الحديثة في الإثبات والتحقيق الجنائي المنعقد في أمستردام في الفترة من (١٠) إلى (١٥) ديسمبر ١٩٩٩م والذي شارك فيه (١٧٠) من العلماء والخبراء ورجال القانون بتأكيد قناعة المشاركين بتخلف الخطط وبرامج تدريب وتأهيل رجال تنفيذ القوانين لعدم قدرتهم على مواكبة مشكلات الإجرام في الألفية الثالثة وخصوصاً الجرائم المعلوماتية، لذا كانت دعوة المؤتمر إلى مزيد من التعليم لهم (عبد المطلب، ٢٠٠١م: ٢).

وإذا كان إثبات الجرائم أمام المحاكم يعتمد على إتباع القواعد الفنية الشرطية من اخذ أقوال الشهود والجاني والمجني عليهم وجمع الأدلة ومعاينة مسرح الجريمة في الجرائم العادية، مما يتطلب خبرات معينة، فإنه لابد من الاستعانة بخبراء نظم المعلومات في الجرائم المعلوماتية لمعاينة مسرح الجريمة ولضبط وفحص آثارها ومعرفة أولويات الأدلة واستنتاج الحقائق ومعرفة الإجابة والرد على المتهم أمام القضاء تحسباً لكون المتهم خبيراً في مجال نظم المعلومات، والاستعانة أيضاً بوسائل التقنية لكشف وتتبع مرتكبي هذه الجرائم ومعرفة أساليب ارتكابهم لهذه الجرائم. لقد أصبح هاجس المؤسسات الإدارية من أجهزة حكومية ومؤسسات تجارية ومؤسسات مالية حماية نظم معلوماتها، بأفضل مستوى ممكن. ولهذا توجب على الأجهزة الأمنية تحمل مسئولية حماية المجتمع من هذه الجرائم وعدم رهن حقوق المجتمع لمؤسسات هدفها تحقيق الكسب المادي بينما هي غير مكلفة بتحقيق العدالة.

في هذه الدراسة سيتناول الباحث أنماط هذه الجرائم وأساليب وأدوات ارتكابها ووسائل التحقيق فيها.

١-٣ مشكلة الدراسة

تواجه نظم المعلومات تهديدات عديدة. فمن داخل المؤسسة هناك احتمال تعرض الملفات للسرقة أو النسخ أو سوء الاستخدام أو تعرض قاعدة البيانات للتغيير أو التزوير، أو التدمير، أو التجسس، كما يمكن أن تفشل إجراءات الحماية والتدقيق، وأيضاً قد تتعطل أجهزه الحماية أو تفشل البرمجيات المستخدمة، ويشكل العاملون في المؤسسة التهديد الأكبر، فالمبرمجون لديهم القدرة على إلغاء أو إفشاء إجراءات الحماية أو إيجاد منافذ خاصة للنظم. والمشغلون لديهم إمكانية تعطيل وسائل الحماية. كما أن مهندسو الصيانة لديهم القدرة على إفساد الأجهزة أو وضع أدوات تنصت أو استخدام برمجيات غير مرخصة (داود، ١٤٢٠هـ: ٣٣). "فالجرائم الداخلية كما تشير الإحصاءات تشكل ما يقارب (٨٠٪) من جرائم الحاسب الآلي" (الفنتوخ، ١٤٢١هـ: ٦٤).

أما التهديدات الخارجية فغالباً ما يكون مصدرها الشبكات، ونظراً لانتقال المعلومات عن طريق أنواع مختلفة من الشبكات السلكية ولا سلكية فإنها عرضة للالتقاط، والاستخدام غير قانوني. كما أن تزايد تعقيدها يوفر أرضية خصبة لتلك الجرائم (العِلم لأمن المعلومات، ٢٠٠٢م).

"فأعداد جرائم نظم المعلومات في ازدياد مستمر وضخامة هائلة، مع انه لا يعلن منها إلا القليل" (داود، أ، ١٤٢٠هـ: ٣٤). فأشهرها تلك التي أطاحت ببنك بارينجز (Bearings Bank) عام ١٩٩٥م في بريطانيا حيث قام أحد مسئولي البنك بعمل استثمارات كبيرة للبنك في سوق الأسهم اليابانية، وبعد سقوط حاد لتلك الاستثمارات حاول إخفاء الخسائر والتي تقدر بحوالي بليون جنيه إسترليني، باستخدام حسابات جانبية وهمية أدخلها في الحاسبات الآلية في البنك فظهر الأمر وكأن الأموال انتقلت من حساب لآخر داخل النظام المعلوماتي للبنك (Parker, ١٩٩٨: ٧٣).

وتشير إحصاءات الجمعية الأمريكية للأمن الصناعي عام ١٩٩٨م إلى أن الخسائر المالية المرتكبة بواسطة الحاسب الآلي للصناعات الأمريكية تبلغ (٦٣) بليون دولار سنوياً، كما يبلغ متوسط

سرقات البنوك بواسطة الحاسب الآلي (١,٥) مليون دولار سنوياً علماً بأن المكتشف من تلك الجرائم لا يتجاوز (١٪) (البشري، ١٤٢١هـ). كما قدرت خسائر المؤسسات التجارية حول العالم نتيجة للهجمات المدروسة التي تصيب نظم المعلومات بمبلغ مائة مليار دولار، وهذا الرقم في ازدياد مستمر (العِلم لأمن المعلومات، ١٤٢٣هـ). كما أن مؤسسات الأعمال الأميركية تكبدت خسائر مالية بقيمة (٤٥٥,٤٨٤,٠٠٠) دولار عام ٢٠٠٢م مقارنة (٣٧٨) مليون دولار تقريباً لعام ٢٠٠١م ومقارنة (٢٦٥) مليون دولار لعام ٢٠٠٠م، كما أن متوسط الخسارة السنوية على مدى ثلاث سنوات قبل عام ٢٠٠٠م كان في حدود (١٣٠) مليون دولار بسبب جرائم نظم المعلومات (Rapalus, ٢٠٠٢). وقد يحمل المستقبل أنواعاً جديدة غير متوقعة من جرائم نظم المعلومات، وقد تكون الحرب القادمة معلوماتية يحاول كل طرف إلحاق الضرر بالآخر عن طريق تدمير البنية المعلوماتية للخصم وإفساد قواعد البينات ونظم المعلومات لما فيها من قيمة استراتيجية عظيمة (داود، ١٤٢٠هـ: ٣٢).

تعد المملكة من أكبر خمسة دول عالمية في معدلات نمو أعداد أجهزة الحاسب الآلي المستخدمة، حيث وصل النمو السنوي إلى (٣٢٪) في عام ٢٠٠٠م، وتعد كذلك أكبر أسواق الشرق الأوسط في أعداد الحاسب الآلي المباعة (الرقابي، ١٤٢٣هـ: ٥٥). ويبلغ عدد مشتركي خدمة الإنترنت في المملكة في أبريل عام ٢٠٠١م (٦٩٠,٠٠٠) ستمائة وتسعون ألف، وتضاعف هذا العدد في ديسمبر عام ٢٠٠٢م ليصبح (١,٤٥٣,٠٠٠) مليون وأربعمائة وثلاثة وخمسون ألف مشترك حسب إحصاءات مدينة الملك عبد العزيز للعلوم والتقنية عن عدد مستخدمي الإنترنت في المملكة، كما يبلغ عدد مستخدمي الإنترنت عبر خطوط الهاتف ما يقارب المليون، ويبلغ مجموع تسجيل أسماء النطاقات في المملكة (٤٥٠٠) أسماً، احتلت أسماء النطاقات التجارية النسبة الأكبر بواقع (٣٣٨٠) اسماً، وتنمو الإنترنت بشكل سريع، بحيث تقدر الإحصاءات نسبة النمو في قطاع الإنترنت في السوق السعودي بـ: (٢٧٦٪)، ليشكل بذلك المركز الرابع عالمياً في مجال الإنترنت، مستحوذاً على (٤٠٪) من سوق المعلوماتية في منطقة الشرق الأوسط (مدينة الملك عبد العزيز للعلوم والتقنية، ١٤٢٣هـ).

تعد جرائم نظم المعلومات من الجرائم المستحدثة باعتبارها جرائم لا تعرف الحدود الجغرافية (البداينة، ١٩٩٧م: ١٤)، الأمر الذي حدا بالمملكة في إطار ثورة التقنية التي يشهدها العالم حالياً بالتطوير وتحديث شبكة الاتصالات الدولية إلى السعي الجاد لملاحقة كل ما هو جديد نظراً لارتباط الجريمة المستحدثة بتلك التقنية الجديدة في عالم الاتصالات والتي يساء استخدامها بما يؤثر على اقتصاديات البلد، خاصة في ظل السعي للدخول في التجارة الإلكترونية بشكل واسع عبر معالجة المعوقات، وأخذت تطبيقات نظم المعلومات في المملكة بالتوسع في مختلف القطاعات، الأمر الذي لم يجعلها بمنأى عن ارتكاب جرائم نظم المعلومات (عالم الكمبيوتر، ١٤٢٣هـ).

يقدر حجم الخسائر المادية لجرائم الحاسب الآلي في المملكة بحوالي (١١٢) مليون ريال سعودي في عام ١٤١٨هـ (البداينة، ١٩٩٨م: ٢٨). كما تقدر تكلفة جرائم الحاسب الآلي في المملكة بحوالي (٥٦٢,٥) مليون ريال، أصابت العديد من المؤسسات والأفراد خلال عام ١٤١٩هـ (البداينة، ١٤٢٠هـ: ٢٨). وزاد انتشار جرائم الحاسب الآلي في المملكة مع انتشار استخدامات الإنترنت فيها وتوفر المعلومات والوسائل التي تسهل عمليات الاختراق وسرقة المعلومات التي أصبحت تمارس من قبل مستخدمي الإنترنت من الداخل والخارج، مما نتج عنه ازدياد أعداد جرائم نظم المعلومات في المملكة رغم التكتم الشديد في الإفصاح عنها من قبل الشركات والمصارف المالية التي تتعرض لمثل هذه العمليات (عالم الكمبيوتر، ١٤٢٣هـ).

وفي مجال التحقيق بجرائم نظم المعلومات تكمن صعوبة اكتشاف هذه الجرائم ومقاضاة المتهم في عدم وجود الخبرة والمعرفة الفنية لدى المحققين في استنتاج الأدلة المثبتة لارتكاب جرائم نظم المعلومات، والذين يحتاجون للمزيد من الخبرة لاستنطاق الأدلة الفنية الموجودة بالحاسب الآلي الشاهد الصامت الأمين وصاحب الذاكرة القوية، الذي يمكن استخدامه للتوصل إلى الجاني. "وأدى نقص المعرفة الفنية والخبرة إلى فشل الكثير من أجهزة الشرطة في ضبط مرتكبي هذا النوع من الجرائم وضبط أدلتها" (رستم، ١٩٩٤م: ١٣)، مما أدى إلى وجود نوع من عدم التكافؤ بين خبرات مجرمي

نظم المعلومات والأجهزة الأمنية الأمر الذي أدى إلى القفزات الكبيرة في مجال جرائم نظم المعلومات (بحر، ١٤٢٠هـ: ٤٧). فالمشكلة التي تتصدى لها هذه الدراسة هي عدم وضوح الوسائل المناسبة للتحقيق في جرائم نظم المعلومات، أو عدم توفرها للمحققين، أو عدم استغلالها بالصورة المناسبة، الذي يتطلب معرفة أساليب وأدوات ومنافذ ارتكاب جرائم نظم المعلومات، وإيضاح وسائل التحقيق المساعدة في توفير الأدلة المثبتة على وقوعها وتحديد شخصية مرتكبها. ويمكن صياغة المشكلة عبر السؤال التالي:

ما هي الوسائل المساعدة على التحقيق في جرائم نظم المعلومات، وكيف تستغل بصورة فاعلة في الوصول إلى مجرمي نظم المعلومات؟

١-٤ أهمية الدراسة

أدت الزيادة المستمرة في استخدام نظم المعلومات في المجالات العلمية والاقتصادية، والاجتماعية، إلى جانب استخدام الإنترنت إلى الزيادة في جرائم نظم المعلومات، فأصبحت جرائم نظم المعلومات متسعة النطاق، باهظة التكاليف وصعبة الرصد والمعالجة. ويمكن بيان الأهمية على النحو التالي:

١. ستكون هذه الدراسة مرجعاً للعاملين في الأجهزة الأمنية في مجال معرفة وسائل التحقيق في جرائم نظم المعلومات وكيفية مساهمتها في تسهيل أعمال التحقيق. وإيضاح الوسائل التي عن طريقها يتم جمع الأدلة المثبتة لوقوع الجرائم، وتحديد شخصية مرتكبها، وتثبت ارتكابها على المتهم.

٢. تقدم للعاملين في مجالات نظم المعلومات إطاراً لكيفية الانسجام مع المتطلبات الأمنية اللازمة لأعمال التحقيق.كما تفيد الجهات المتضررة من هذه الجرائم في وضع سياسة أمنية شاملة لحماية نظم معلوماتها.

٣. تسهل وضع سياسة تدريبية للعاملين في أمن المعلومات ليتمكنوا من تحقيق أمن المعلومات وذلك بمعرفة مستوى الأمن لديهم، والاطلاع على أساليب وأدوات ومنافذ ارتكابها.

٤. تسهل وضع سياسة تدريبية للعاملين في الأجهزة الأمنية ليتمكنوا من التحقيق بتلك الجرائم باستخدام وسائل التحقيق المبينة على أسس علمية محددة، ليكونوا قادرين على مواجهة تحديات التطور الهائل في أساليب ارتكاب هذه الجرائم.

٥. تساهم هذه الدراسة بلفت انتباه العاملين بالأجهزة الأمنية بشكل خاص والباحثين بشكل عام إلى خطورة جرائم نظم المعلومات التي تتطلب المواجهة بوسائل حديثة، وتحتاج إلى مزيد من البحث والدراسة، كما تقدم مرجعاً علمياً يساهم في إثراء المكتبة العربية في مجال جرائم نظم المعلومات.

١-٥ أهداف الدراسة

١. وضع إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات.
٢. تحديد الإجراءات الأمنية سواء كانت فنية أو إدارية لتحقيق أمن نظم المعلومات.
٣. تحديد أنماط جرائم نظم المعلومات ومدى حدوثها بالمؤسسات وأضرارها ودوافعها.
٤. حصر الأساليب المستخدمة في ارتكاب جرائم نظم المعلومات ومنافذها.
٥. حصر الأدوات المستخدمة من قبل مجرمي نظم المعلومات وكيف يمكن لمجرمي نظم المعلومات بالمملكة أن يحصلوا عليها.
٦. الكشف عن وسائل التحقيق في جرائم نظم المعلومات.
٧. بيان العوائق التي تحول دون استخدام تلك الوسائل.
٨. تحديد أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات.

١-٦ أسئلة الدراسة وفرضياتها

تهدف هذه الدراسة إلى تحديد وسائل التحقيق في جرائم نظم المعلومات من خلال الإجابة على أسئلة الدراسة وفحص فرضياتها.

١-٦-١ أسئلة الدراسة

١. ما العناصر المكونة للسياسة الأمنية لأمن المعلومات وما مدى وضوح تلك العناصر بالمؤسسات؟
٢. ما الإجراءات الفنية والإدارية لتحقيق أمن نظم المعلومات وما مدى إتباعها من قبل المؤسسات؟
٣. ما أنماط جرائم نظم المعلومات، وما مدى حدوثها بالمؤسسات، وأضرارها، ودوافعها؟
٤. ما الأساليب المستخدمة في ارتكاب جرائم نظم المعلومات، ومنافذها؟
٥. ما الأدوات المستخدمة من قبل مجرمي نظم المعلومات، وكيف يمكن أن يحصلوا عليها بالمملكة.
٦. ما وسائل التحقيق في جرائم نظم المعلومات؟
٧. ما العوائق التي تحول دون استخدام تلك الوسائل؟
٨. ما أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات؟

١-٦-٢ فرضيات الدراسة

١. لا توجد علاقة ذات دلالة إحصائية بين التزام المؤسسة بتحديث برامجها وبين اكتشاف الجرائم التي تتعرض لها.

٢. لا توجد فروق ذات دلالة إحصائية بين متوسط أراء كل من المحققين، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن نظم المعلومات حول وسائل التحقيق.

٣. لا توجد فروق ذات دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول مدى الموافقة على وجود عوائق استخدام وسائل ضبط الجريمة والتحقيق فيها.

١-٧ التعريفات الفنية والإجرائية

١-٧-١ النظام System

"يُعرف بأنه مجموعة من العناصر أو المكونات التي تتفاعل مع بعضها البعض لتحقيق هدف محدد" (برهان، ١٩٨٩م: ٣). كما "يُعرف بأنه مجموعة من الإجراءات لدعم اتخاذ القرار والتحكم بالأعمال" (الحويطى، ١٤٢٢هـ: ٢٨).

١-٧-٢ المعلومات Information

يمكن تعريف المعلومات "بأنها البيانات والحقائق والأرقام، والأوصاف التي تساعد الإدارة على تصور ما يحدث من ظواهر وأحداث وصولاً إلى التنبؤ الدقيق بما يمكن أن يحدث في المستقبل ومن ثم يكون في إمكان الإدارة تعظيم قدراتها على إجراء الاتصالات الإدارية، واتخاذ القرارات، ورسم الخطط الملائمة، والرقابة على مختلف أوجه النشاط" (المصري، ١٩٨٩م: ٢٠٢).

١-٧-٣ البيانات Data

هي ما يستخدم لوصف فكرة أو حدثٍ أو موضوع أو هدفٍ أو أي حقائق أخرى، ويمكن النظر إليها على أنها المادة الخام التي يتم ترتيبها وتنظيمها للحصول على فائدة أكثر (خشبة، ١٩٩٣م: ٥٥).

١-٧-٤ نظام المعلومات Information System

هي "مجموعة من الإجراءات والبرامج والأفراد والأجهزة والاتصالات وقاعدة البيانات التي تهدف إلى إنتاج معلومات محددة" (غراب، وحجازي، ١٩٩٩م: ٩٠).

١-٧-٥ السياسة الأمنية Security Policy

هي كل ما يتعلق بوضع لوائح وقوانين تتبع لمواجهة الجرائم التي ترتكب بواسطة الحاسب الآلي, أو عبر شبكاته, وتحديد أنواعها, ومدلولاتها الأمنية, وكيفية ارتكابها, والحماية الجنائية

لمحتوياتها، وتطبيق الإجراءات الفنية لأمن برامجها, وأمن الاتصالات في شبكاتها, والإجراءات الإدارية لأمن استخدامها.

١-٧-٦ أمن المعلومات Information Security

حماية أصول وموارد نظام ما بطرق مشروعة بتنظيم العلاقات والاتصالات داخل النظام دون أن يؤثر على الأداء في النظام، وهو لا يمنع الجريمة نهائيا، ولكن كلما كان النظام الأمني قوياً ودقيقاً كانت الجريمة أقل تكلفة وأسرع في الكشف (مدينة الملك عبد العزيز للعلوم والتقنية، ١٤٢٣هـ).

١-٧-٧ الجريمة Crime

التعريف الشرعي للجريمة هو " إتيان فعل محرّم معاقب على فعله، أو ترك فعل محرّم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه " (عوده، ١٤٠١هـ: ٧٦). وأما التعريف القانوني للجريمة فهو" عمل إي عمل يجرِّمه القانون، أو امتناع عن عمل يقضى به القانون، ولا يعد الفعل أو الترك جريمة في نظر القوانين إلا إذا كان معاقباً عليه طبقاً للتشريع الجنائي " (عوده، ١٤٠١هـ).

١-٧-٨ جريمة نظم المعلومات Information Systems Crime

هي؛ جميع الجرائم التي تكون نظم المعلومات هدفها أو التي يتم ارتكابها بواسطة نظم المعلومات (البيانات، والمعلومات، والبرامج، وأجهزة الحاسبات الآلية والأجهزة الملحقة بها، وقاعدة البيانات، والاتصالات، والشبكات بما فيها الإنترنت) بطرق ووسائل مختلفة سواء كان من داخل المؤسسة أومن خارجها (عن طريق منسوبيها أو أفراد آخرين)، للقيام بتلاعب وإفساد أو تخريب أو سرقة أو أي عمل أخر غير مشروع يرتكب بواسطة نظم المعلومات، مما يتسبب بإلحاق الضرر بالنظام المعلوماتي لمؤسسة بشكلٍ كامل أو جزء من نظامها.

١-٧-١٠ التحقيق Investigation

"هو البحث عن الحقيقة، وفي المجال الجنائي الجهد المبذول لكشف غموض الجرائم وتحديد شخصية مرتكبيها، واثبات التهمة عليهم بما يقدم من أدلة إثبات" (عبد الحميد، ١٤٢٠هـ: ١٢).

١-٧-١١ وسائل التحقيق Investigation Tools

هي تلك الأدوات التي تنطلق الحاجة إليها من طبيعة جرائم نظم المعلومات بأن مرتكبها غالباً مجهول الهوية، مما يتطلب من المحقق إتباع طرق متعددة للوصول إلى الجاني وذلك بإتباع الوسائل التي تحقق من شخصية الجاني وذلك بمعرفة أسلوبه في ارتكاب الجريمة والأداة التي ارتكب بها الجريمة، ووصف الأشياء التي وقعت عليها الجريمة والمتمثلة في أسلوب عمل النظام وحمايته، وهدف الجاني من الجريمة، وجميع الأدوات التي تؤدي إلى ضبط جريمته والتعرف عليه وتوفير الأدلة المثبتة شريطة أن تكون تلك الوسائل في نطاق المشروعية.

١-٧-١٢ الأدلة Evidences

"براهين قائمة على المنطق والعقل، في إطار من الشرعية الإجرائية لإثبات صحة افتراض، أو رفع أو خفض درجة اليقين الإقناعي في واقعة محل خلاف" (أبو القاسم، ١٤١٤هـ: ١٨٤). "كما تُعرف بأنها الوقائع المادية أو المعنوية التي تتصل بالجريمة ويؤدي اكتشافها إلى تحديد كل أو بعض أبعاد الجريمة مثل وقتها ومكانها ودوافعها، وأسلوب ارتكابها والظروف المحيطة بها ومسئولية أطرافها من متهمين ومجني عليهم" (عبد الحميد، ١٤٢٠هـ: ١٨٤).

١-٧-١٢ الأدلة الإلكترونية Electronic Evidences

"هي معلومات يقبلها المنطق ويعتمدها العلم، ويتم الحصول عليها بإجراءات قانونية علمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاته وشبكاته، ويمكن استخدامها

في أي مرحلة من مراحل التحقيق لإثبات حقيقة متعلقة بأحد أطراف الجريمة" (البشري، ١٤٢٣هـ: ١٣٣).

١-٧-١٣ الإثبات الجنائي Criminality Identity

"كل ما يؤدي إلى إظهار الحقيقة لأجل الحكم على المتهم، ولابد من ثبوت وقوع الجريمة في نفسها وأن المتهم هو المرتكب لها بوجود دليل يثبت ارتكابه للجريمة" (أبو القاسم، ١٤١٤هـ: ٨١).

١-٧-١٤ الأجهزة الأمنية Security Administration

"هي المؤسسات المنوط بها العمل لسيادة النظام وفرض هيبته" (أبو شامة، ١٩٩٢م: ١٠١).

١-٧-١٥ الاختراق Hacking

هو القدرة على الدخول إلى نظام معلوماتي عن طريق منافذ في نظام الحماية بغض النظر عن الأضرار التي قد يحدثها (مجلة الأمن الإلكترونية، ٢٠٠٢م).

١-٧-١٦ الفيروسات Virus

هي برامج صغيرة تصيب الأجهزة وتتسبب في الكثير من المشاكل كمسح الذاكرة أو مسح بعض الملفات الهامة في نظم التشغيل أو القيام بإصدار الأوامر لبعض البرامج بدون تدخل مباشر من قبل المستخدم (مجلة الأمن الإلكترونية، ٢٠٠٢م).

١-٧-١٧ البرنامج Program

"مجموعة من الأوامر والتعليمات التي تسمح بعد تحويلها إلى لغة الآلة القادرة على معالجة المعلومات بإنجاز وظيفة معينة على أن تكون هذه الأوامر والتعليمات مشفوعة بوصف البرنامج والمستندات التي تبسط فهمه وتيسير تطبيقه" (شتا، ٢٠٠١م: ٤٤).

١-٧-١٨ ديدان الإنترنت Internet Worms

هي شبيهة جداً بالفيروسات ولكنها تختلف في الهدف حيث تقوم بمسح أو تدمير المعلومات من البرامج التطبيقية كبرامج المحاسبة وقواعد المعلومات فقط كما أن بمقدور هذه الديدان التكاثر حتى تملأ الذاكرة وتعطل الأجهزة (مجلة الأمن الإلكترونية، ٢٠٠١م).

١-٧-١٩ أحصنة طروادة Trojan Horses

هي برامج لتتجسس تقوم بجمع المعلومات والبيانات ومن ثم إرسالها لمصدرها (مرسل برنامج حصان طروادة) وعادة ما يكون فرد أو موقع أو مؤسسة لجمع المعلومات (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

١-٧-٢٠ جدار الحماية Firewall

"أداة تصفي أو تحجز مرور البيانات بين الشبكة المحمية والخارجية لحجز كل غير مرغوب فيه بتطبيق سياسة أمنية معينة" (داود، ب، ٢٠٠٠م: ٢٣٠). كما تعرف بأنها نظام أمني لتنظيم حركة المرور عند نقاط الاتصال بين الشبكات (إنترنت العالم العربي، ١٤٢٣هـ).

١-٨ خلاصة الفصل الأول

في هذا الفصل تم استعراض مشكلة الدراسة والتي تركز على عدم وضوح الوسائل المناسبة للتحقيق في جرائم نظم المعلومات، أو عدم توفرها للمحققين، أو عدم استغلالها بالصورة المناسبة. وتعد دراسة هذا الموضوع مهمة، لما قد توفره للعاملين في مجال التحقيق في جرائم نظم المعلومات من تصور واضح عن تلك الوسائل وكيفية مساهمتها في تسهيل أعمال التحقيق. كما ستقدم للعاملين في مجالات نظم المعلومات إطاراً لكيفية الانسجام مع المتطلبات الأمنية اللازمة لأعمال التحقيق، وما قد تفيد به الجهات المتضررة من هذه الجرائم في وضع سياسة أمنية لحماية نظم معلوماتها.

الفصل الثاني/ نظم المعلومات

٢ـ١ المقدمة

نظراً لكون نظم المعلومات مستهدفة في ارتكاب جرائم نظم المعلومات وما يتطلبه التحقيق من الاطلاع على أجزاء النظام المعلوماتي كقاعدة البيانات والشبكات وإدارتهما، ومعرفة موارد النظام، والمستفيدين، فسوف يتم تناول المعلومات لأنها الهدف الرئيسي من إنشاء النظام المعلوماتي. لذا سوف يتم عرض لنماذج من نظم المعلومات، وتوضيح مكونات تلك النظم من أجهزة حاسبات آلية، وبرامج، وقواعد بيانات، وشبكات وأفراد.

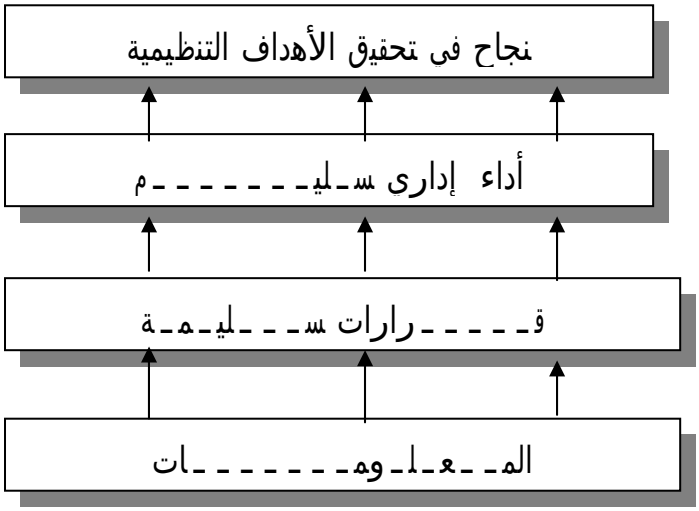
٢ـ٢ المعلومات

٢ـ٢ـ١ أهمية المعلومات

تعد المعلومات من المصادر القومية المؤثرة في تطور ونمو المجتمعات، حيث أن الدول المتقدمة تعدها كالمصادر الطبيعية الأخرى من حيث الأهمية. "لذلك أصبحت المعلومات قاعدة أساسية لأي تقدم حضاري أو علمي أو صناعي في أي مجتمع، فبدون المعلومات لا تستطيع الدول أن تتقدم أو حتى تستطيع أن تحافظ على تقدمها" (يونس، ١٩٨٩م: ٩). وتلعب المعلومات دوراً حيوياً وهاماً في كفاءة الأداء في المؤسسة مما تطلب من المؤسسات إنشاء نظم معلومات تساعدها بالقيام لأداء وظائفها بنجاح وكفاءة عالية، شكل رقم (١) (الحازمي، ١٤٢٠هـ: ٢٣). كما تنبع أهمية المعلومات لكونها أهم الموارد في المجتمع، فهي القوة التي تعتمد عليها الدول بعد أن تطورت التقنية التي جعلت منها ذات قيمة حيوية وزادت من القدرة على استخدامها في مجالات عدة. وبازدياد حجم المعلومات زادت الحاجة إلى تبادلها بين المؤسسات أو الدول ولذا ظهرت ثورة الاتصالات، بعدها ظهرت الاتصالات الرقمية، وزاد التطور بعد ذلك بظهور شبكات المعلومات التي انتشرت في كل مكان

بتقنياتها المختلفة وأنواعها المتعددة، وسهلت الأقمار الاصطناعية انتقال المعلومات دون الحاجة إلى أسلاك وأطباق (داود، أ، ٢٠٠٠م: ٢٠٧). وأخيراً ظهور الإنترنت الذي ضاعف من حجم المعلومات وسهل من تبادلها وصعب من الرقابة على انتقالها مما سنح باستغلالها لتحقيق أهداف غير مشروعة.

شكل رقم (١) أهمية المعلومات في الإطار التنظيمي



المصدر: (باجابر والمفتي، ١٤٠٧هـ) (موثق في الحازمي، ١٤٢٠هـ: ٢٣)

٢-٢-٢ حرب المعلومات

بعد التضخم الكبير في صناعة المعلومات جعل الاعتماد على نظم المعلومات أكبر في إدارة جميع القطاعات المختلفة، ولذا فإن استخدام المعلومات كسلاح أصبح أكثر عنفاً وأشد تأثيراً، وتعطل تلك النظم يعد أمراً مخيفاً (ومشكلة الصفرين عام ألفين أكبر دليل على ذلك)، فبعد ظهور الحاسب الآلي واستخدام الشبكات وانتشار شبكة الإنترنت واتساع استخدامها بدأت حرب المعلومات تأخذ بعداً جديداً (الهاجري، ١٤٢٣هـ). ولقد نقل الهاجري عن (Denning) "أنه في حرب الخليج الثانية تم استخدام وسائل حديثة في المعركة المعلوماتية، حيث استخدمت الأقمار الصناعية، وطائرات التجسس المختلفة، وقد تزامن مع ذلك قيام مجموعة من المخترقين الهولنديين، باختراق عدد كبير من أجهزة الحاسب الآلي التابعة للدفاع الأمريكي مرتبطة بشبكة الإنترنت، كانت تحتوي على معلومات هامة عن

الجيش الأمريكي، واستطاعوا معرفة معلومات حساسة مثل مواقع الجيش وتفاصيل الأسلحة المختلفة الموجودة في كل موقع من هذه المواقع، وكان يمكن أن يستغلها النظام العراقي لصالحه" (الهاجري، ١٤٢٣هـ). كما نقل الهاجري عن (Wired) بأنه يمكن أن يكون الهجوم على المعلومات مصاحباً لحرب تقليدية أو نتيجة رد فعل لاعتداء كالذي حدث بين مجموعات عربية و إسرائيلية من المخترقين في عامي ٢٠٠٠م و٢٠٠١م حيث قام كل طرف بتعطيل أو تخريب مواقع للطرف الآخر وحصيلة حرب نظم المعلومات تخريب (٤٠) موقع إسرائيلي مقابل (١٥) موقع عربي (الهاجري، ١٤٢٣هـ).

وتستهدف حرب المعلومات عند الطرف الأخر المعلومات ونظمها للاستحواذ عليها أو تقليل قيمتها أو وتخريبها أو تعطيل أجهزتها أو سرقة أو تشويه معلوماتها، لأهداف تجارية بين المؤسسات أو إستراتيجية أو عسكرية بين الدول، أو التعدي على الملكية الفكرية وقرصنة المعلومات كسرقة البرامج وتوزيع مواد مكتوبة أو مصورة بدون إذن المالك الشرعي، وغيرها من الأهداف العامة والخاصة (الهاجري، ١٤٢٣هـ).

٢-٢-٣ مجتمع المعلومات

تتجه الدول إلى التنمية في مجال تقنية المعلومات وتحويل المجتمع ومؤسساته إلى مجتمع معلوماتي، وتحقق التنمية في مجال تقنية المعلومات زيادة القدرة التنافسية للمنتجات ودعم الأسواق كمجال التجارة الإلكترونية، وكذلك الحكومة الإلكترونية، فتدعم إنشاء مؤسسات لتقنية المعلومات ترعى الأعمال الإلكترونية، وتحاول وضع الاستراتيجيات الواضحة لتقنية المعلومات التي أصبحت مدخلاً هاماً لتحقيق معدلات نمو عالية (جويلي، ١٤٢٣هـ: ١٨). كما تعمل تلك الدول على تحديث هياكلها لمواكبة عصر المعرفة والمعلومات، بإقامة صناعة معلومات واتصالات على مستوى عال، وصياغة الإطار التشريعي اللازم للبيئة التقنية الجديدة إلى جانب استكمال البنية التحتية في مجال تقنية المعلومات (المعيلي، ١٤٢٣هـ:١١).

يواجه مجتمع المعلومات تحديات متعددة، كالتحدي البشري الذي يتضمن إعداد الكوادر الفنية المدربة والمؤهلة للعمل في إطار هذه المؤسسات، وإلى جانبه التحدي الصناعي الذي يتمثل في قيام صناعة قوية ذات أساس راسخ في هذا المجال، ويواجه عدم صياغة السياسات والحوافز اللازمة لتشجيع ازدهار المؤسسات التي تعتمد على تقنية المعلومات، وتزيل جميع المعوقات التي تواجها تلك المؤسسات. كما يواجه عدم وجود أراء واضحة في مجال تقنية المعلومات، وعدم ترجمة هذه الرؤى إلى مبادرات تتمثل في تعليم وتأهيل البشري، ورفع الفعالية الحكومية وخدمة حلول للمشاكل البشرية، وتحسين الخدمات من خلال تطوير فكر وبنية المؤسسات القائمة، حتى تستطيع تحقيق الأهداف المرجوة منها، ومن خلال التحول للحكومة الإلكترونية, واعتماد التجارة الإلكترونية، وتحقيق العدالة المعلوماتية (الشريف، ١٤٢٣هـ: ٢٤).

٢-٣ نماذج نظم المعلومات

يهدف النظام المعلوماتي بشكل عام إلى الاستفادة من البيانات المتوفرة بقواعد البيانات وتحويلها إلى معلومات، والحصول على المعلومات مباشرة بواسطة المستفيد الأول، كما يهدف إلى المساعدة على اتخاذ القرارات المستندة على المعلومات، والقدرة على الحصول على المعلومة الصحيحة وذلك بتطبيق مبدأ التكامل بين مختلف قواعد المعلومات، وتطبيق مبدأ الجودة الشاملة، وتيسير إجراءات العمل (جامعة الملك عبد العزيز، ١٤٢٣هـ). وفيما يلي بعض من نماذج نظم المعلومات.

٢-٣-١ نظام المعلومات الإدارية

تضم نظم المعلومات الإدارية Management Information Systems مجموعة واسعة من التطبيقات الموجهة لتلبية الاحتياجات المعلوماتية للإدارة في مختلف المستويات، وتستخدم هذه النظم في وظائف الإدارة المختلفة (الإنتاجية، والمالية، وإدارة المواد، والمحاسبية، وإدارة المخزون،

ومعالجة الطلبات، والتسويق) وعلى جميع مستويات الإدارة (عليا، وسطى، تنفيذية) لكي تقوم بأداء الوظائف الإدارية (تخطيط، تنظيم، توجيه، رقابة) (الحويطى، ١٤٢٢هـ: ٣٧) حتى تحقق الإدارة أهدافها.

٢-٣-٢ نظم معالجة العمليات

يقصد بنظم معالجة العمليات Transaction Processing Systems الوقائع أو الأحداث التي تتم في بيئة المؤسسة وتؤثر في سيرها نحو تحقيق أهدافها. فمثلا عمليات البيع والشراء أو استلام فاتورة أو تنظيم شيك أو غير ذلك، تمثل عمليات يومية تتم في المؤسسة، وفور حدوث هذه العمليات، يجب التقاط البيانات الناتجة عنها، وتسجيلها وإدخالها إلى الحاسب ليتم معالجتها بواسطة نظم معالجة العمليات (الحويطى، ١٤٢٢هـ: ٣٨) ومن أهم تطبيقاتها القطاعات المصرفية والمالية.

٣-٣-٢ نظم دعم القرارات

تهدف نظم دعم القرارات Decision Support Systems إلى مساعدة المدراء في اتخاذ القرارات المتعلقة بالحالات قليلة الحدوث، حيث يكون من الصعوبة إمكانية التحديد المسبق للمعلومات اللازمة لاتخاذ هذه القرارات. وتتصف هذه القرارات عموماً بعدم وضوح البنية (أي صعوبة تحديد متغيرات القرار وعلاقتها بالهدف المطلوب والوصول إليه). وتعد هذه النظم مهمة بشكل خاص بالنسبة للإدارة العليا في المؤسسة التي تتعامل بشكل دائم مع القضايا الإستراتيجية والتي تتطلب طبيعة عملها اتخاذ القرارات في الحالات الطارئة وغير المتوقعة (برهان، ورحّو، ١٩٩٨: ٤١).

٤-٣-٢ نظم المعلومات الصحية

يربط النظام المعلوماتي الصحي Health Information Systems جميع أقسام المستشفى وبقية المستشفيات الأخرى بالمناطق المختلفة بعضها مع بعض، بحيث يتم إدخال جميع المعلومات الطبية من تحاليل ونتائج أشعة ومختبر والتقارير طبية، وكتابة وصفات طبية والتأكد من عدم تعارض

الأدوية المصروفة التي يأخذها المريض وخصوصا عند ما يراجع أكثر من وحدة طبية. وتجعل نظم المعلومات من المستشفى بدون ملفات ورقية أو أوراق لصرف الأدوية أو طلب الفحوصات (الربيعة، ١٤٢٢هـ: ١٠). وتنظم أعمال الصيدليات، والمختبرات، ونظام التغذية في المستشفيات (الحماحمي، ١٤١٩هـ: ١٢١). كم تأمن نظم المعلومات السرية لمعلومات المرضى أفضل من الملفات الورقية، وتفيد نظم المعلومات عند تنقل المريض من مستشفى ألي أخر توفر المعلومات عنة بدون الحاجة إلى إعادة الفحوصات وبذلك يكون اختصار للجهد وخفض التكلفة المادية وإراحة المريض وتخفيف الضغط على المستشفيات (الربيعة، ١٤٢٢هـ: ١٠). كما تستخدم المستشفيات أجهزة تعتمد على نظم المعلومات في عملها فقد تحدث كوارث بسبب أخطاء فنية أو أخطاء بشرية مقصودة أو غير مقصودة.

٢-٣-٥ نظم المعلومات الجغرافية

تعد نظم المعلومات الجغرافية Geographic Information Systems (GIS) مجموعة منظمة من الحاسبات الآلية والعتاد والبرمجيات والبيانات الجغرافية والموظفين، مصممة لالتقاط وتخزين وتحديث ومعالجة وتحليل وعرض البيانات ذات الأساس الجغرافي (الجودي، ٢٠٠٢م).

٢-٣-٦ النظم الخبيرة

يطلق على النظم الخبيرة Expert Systems نظم الدعم الذكية أو الذكاء الاصطناعي Artificial Intelligence Oriented يقصد بالذكاء الاصطناعي بشكل عام تعليم الحاسب الآلي أداء المهام المختلفة بطريقة ذكية . وليس من خلال تنفيذ سلسلة من التعليمات التي يقوم بتنفيذها بطريقة صماء. وستوفر البرامج المعتمدة على الذكاء الاصطناعي إمكانية ربط الحقائق والقواعد والظروف والحالات المختلفة وتحديد العمليات المناسبة، تتعامل النظم الخبيرة مع الحالات التي تتصف بأقصى حدود عدم التأكد. ولذلك فإن هذه النظم تركز عادة على موضوعات محددة وضيقة جداً، وتجمع القواعد المعرفية والافتراضات والحقائق المتوفرة عنها وتستخدمها للقيام بعمليات الاستنتاج والاستدلال المنطقيين للوصول إلى القرار المطلوب (الحوبطى، ١٤٢٢هـ: ١٢٦).

٢-٣-٧ نظم المعلومات الدفاعي

أصبحت الحاسبات الآلية والتقنيات المصاحبة لها كالشبكات ووسائل الاتصالات من الأساسيات التي تعتمد عليها القوات المسلحة في جميع أجهزتها من الأسلحة البرية، والجوية، والبحرية، والدفاع الجوي، من والصواريخ، ورادارات بدرجة كبيرة. ومع التطور التقني السريع في الوسائل الحربية. على سبيل المثال تمتلك القوات المسلحة الأمريكية ما يزيد على (٥٨٪) من أجهزة الحاسبات الآلية المستخدمة في الحكومة، كما قدرت ميزانية نظم المعلومات لعام ١٩٨٨م بمبلغ (١٧،٤) بليون دولار (الحماحمي، ١٤١٩هـ: ١٣٣).

ولتطوير معدات وبرامج الحاسب الآلي في نظم المعلومات الدفاعية قامت بإنشاء وكالة مشاريع الأبحاث الدفاعية المتقدمة DARPA بهدف دعم المشاريع الجديدة الأبحاث العسكرية وتطوير نظم المعلومات، وفي عام ١٩٨٣م قامت DARPA بتزويد أجهزة الدفاع في الولايات المتحدة الأمريكية بتقنيات الذكاء الصناعي ومن هذه التقنيات الآليات والعربات التي تستطيع العمل في الأماكن الصعبة وتعمل بالروبوت ويصل بعدها (٥٠) كيلو بسرعة (٧٠) كلم/ ساعة، وكذلك مساعد الطيار، وإدارة وتقييم المعركة، ومحاكاة الحروب. وأصبح الاعتماد الكبير على نظام المعلومات الدفاعي Defense Information Systems يثير المخاوف لدى الدول خوفاً من وقوع أخطاء فنية وبشرية، أو استغلال هذه التقنية للهجوم من قبل الخصوم (الحماحمي، ١٤١٩هـ: ١٣٤).

٢-٤ مكونات نظم المعلومات

يتكون نظام المعلومات من حاسبات الآلية، وبرامج، وقاعدة بيانات، وشبكات، وأفراد متخصصين في جميع تخصصات النظام، بهدف إنتاج معلومات يتم من خلال تنفيذها توفير معلومات تستخدم لدعم عملية القرار (غراب، وحجازي، ١٩٩٩م: ٩٢)، كما يتكون من إجراءات تضعها المؤسسات للحصول على البيانات وإدخالها ومن ثم معالجتها وثم إخراجها على شكل معلومات

تساعدها في اتخاذ قرارات دقيقة وسريعة لتنفيذ أعمالها ومن ثم تحقيق أهدافها (الحويطي، ١٤٢٢هـ: ٥٢). وفيما يلي سوف يتم استعراض مكونات نظم المعلومات.

٢.٤.١ الحاسبات الآلية

تعد الحاسبات الآلية أحد المكونات الرئيسية بالنظام المعلوماتي، وتتكون من؛ وحدة المعالجة المركزية CPU (Central Processor Unit)، ويتركز دورها في قراءة وكتابة محتويات الذاكرة، ونقل المعلومات بين خلاياها وخانات التسجيلregister، كما تقوم بترجمة وتنفيذ الأوامر الموجودة في البرامج. وتتكون وحدة المعالجة المركزية من وحدة تسمى بوحدة المنطق والحساب ALU (Arithmetic And Logic Unit) وتقوم بالعمليات الحسابية. ومن وحدة التحكم CU (Control Unit) وتؤدي وظيفة القيادة والسيطرة، حيث تستقبل من الذاكرة وتفسر وتوجه وحدة الحساب أو الوحدات الأخرى لتنفيذها، وتسترجع تعليمات البرنامج واحد بعد أخر، وتقوم بتفسير هذه التعليمات وإصدار التوجيهات (برهان، ورحّو، ١٩٩٨م). كما تتكون وحدة التحكم CU (Control Unit) من ذاكرة الوصول العشوائي RAM (Random Access Memory) (غراب، وحجازي، ١٩٩٩م: ١١٢).

كما تتكون الحاسبات الآلية من وحدة التخزين الرئيسية، التي تقوم بالتخزين المؤقت للمعلومات، وتفقد المعلومات الموجودة فيها عند انقطاع الكهرباء، وذاكرة القراءة فقط ROM (Read Only Memory) وتحتفظ بالمعلومات التي تكتب وقت التصنيع (غراب، وحجازي، ١٩٩٩م: ١١٦)، ولها القدرة على الاحتفاظ بالمعلومات حتى عند انقطاع الكهرباء عنها، ولكن يوجد أنواع منها يمكن مسح محتوياتها والكتابة فيها من جديد وتسمى EPROM أي ذاكرة القراءة فقط والقابلة للمسح والبرمجة، وتم تطويرها EEPROM لتصبح ذاكرة القراءة فقط القابلة للمسح والبرمجة بالكهرباء، هذا بالإضافة إلى ذاكرة Cache Memory والمصممة لأجل تخزين البيانات الضرورية، ومن ثم نقلها إلى وحدة المعالجة المركزية CPU بسرعة تفوق ذاكرة الوصول العشوائي RAM (Nooraelectronics, ٢٠٠٢).

كمـا يتبـع الحاسـب الآلـي أجهـزة الإدخـال Input Devices كلوحـة المفـاتيح Keyboard، والفأرة Mouse، والماسح الضوئي Scanner، وأجهزة تمييز رموز الحبر المغنطيسي MICR وهو من التقنيات المستخدمة غالباً في القطاعات المصرفية، وأجهزة الإدخال الضوئي للبيانات، والقارئات أو الماسحات الرقمية، وأجهزة قراءة الرقع المغناطيسيةMagnetic Stripes Readers، وأجهزة الإدخال الصوتي Voice Input، ويقوم معالج البيانات بالتخاطب مع هذه المنافذ عن طريق شريحة تسمى بشريحة منفذ المدخل والمخرج Input/Output Port Chip (Arabcomputing, ٢٠٠٢).

أمـا أجهـزة الإخـراج Output Devices فهـي كالشاشـة Monitor، والطابعـة Printer بنوعيهـا المتسلسلة والسطرية، وأجهزة الإخراج الميكروفيلمية COM، أجهزة الإخراج الصورية Pictorial Output Devices، والمخرجـات الصـوتية Voice Output، والمحطـات الطرفيـة Terminal هـي محطـات طرفيـة ذات غرض عـام General Purpose Terminal وتنقسم إلـى محطـات طرفيـة ذكيـة Intelligent Terminal ومحطـات طرفيـة عاديـة Dummy Terminal، أو هـي محطـات طرفيـة ذات غرض خـاص Special Purpose Terminal ومن أهم تطبيقاتها محطـات نقـاط البيع POS المزودة بماسح للشفرة العمودية Bar Code Scanner لقراءة أرقام السلع، والصراف الآلـي Teller Machine، وأجهزة التجسس Sensors التي تلتقط المعلومات من محيط ما وترسلها مباشرة إلى الحاسب الآلي (Arabcomputing, ٢٠٠٢).

أما وحدات التخزين الخارجية Storage Units فقد دعت الحاجة إلى صنع تلك الوسائل بحيث تكون في نفس الوقت عملية واقتصادية، لأنه لا يمكن الاعتماد على الذاكرة الموجودة في الحاسب الآلي لحفظ المعلومات، ومن أهم هذه الوسائل الأشرطة الممغنطة، الأقراص الممغنطة التي تتفاوت من حيث سعة تخزين، وسرعة الوصول، وإمكانية النقل وطبيعة القرص مرن Floppy Disk، وقرص

مدمج، وتستقبل هذه الوسائل التخزينية الملفات والتي تتكون من عدد من خلايا التسجيل كل منها بحجم ثابت، وكل خلية قادرة على تخزين معلومات وبرامج (برهان، ورحّو، ١٩٩٨م: ٦٣).

٢-٤-٢ البرامج

تتكون البرامج من عدة أنواع. فبرامج نظم التشغيل OS (Operation System) هي "مجموعة من البريمجات Software المعقدة يتواجد بعضها في الذاكرة بشكل دائم أثناء عمل الحاسب الآلي ليراقب كل ما يقوم به من عمليات ويعرف ببرنامج المشرف Supervisor، وعند البدء بتشغيل الحاسب الآلي لأول مرة يتم تحميل نظام التشغيل إلى الذاكرة سوء من القرص الصلب أو قرص مرن وتسمى System Initialization " (غراب، وحجازي، ١٩٩٩م: ١١٧).

ففي الحاسب الآلي المايكروي يوجد نظام التشغيل مخزناً فقط في ذاكرة القراءة ROM فقط ويتم تحمليه آلياً، وفي الحاسبات الآلية الكبيرة بعد تشغيله تبدأ المكونات المادية بالبحث عن نظام التشغيل وتنفيذه (غراب، وحجازي، ١٩٩٩م: ١١٧). وتعد أهم وظائف نظم التشغيل التحكم بالإدخال والإخراج، وإدارة العمل وإدارة الملفات، وإدارة المكتبات والاتصالات وبرامج التشارك في الموارد والاستفادة القصوى من نظام الحاسب الآلي، ويتم تطوير نظم التشغيل من قبل المؤسسات المنتجة للمكونات المادية للحاسب الآلي (برهان، ورحّو، ١٩٩٨م: ٦٩).

أما البرامج التطبيقية Application Software فتقوم بتوجيه الحاسب الآلي لتنفيذ المهام التي يتطلبها عمل المستخدم مثل معالجة طلبات المبيعات، أو إجراء عمليات الحجز في رحلات الطيران، أو معالجة النصوص أو أعداد وطباعة الفواتير أو غيرها. وتسمى مثل هذه المهام التي ينفذها الحاسب الآلي بالتطبيقات، أما البرامج التي توجه الحاسب الآلي لتنفيذ هذه المهام فتسمى بالبرمجيات التطبيقية. تتعامل البرمجيات التطبيقية مع نظام التشغيل ويتعامل المستخدم بشكل مباشر مع هذه البرمجيات التطبيقية، وبينما يقوم نظام التشغيل بالتحكم في استخدام الحاسب الآلي فإن البرمجيات التطبيقية

تضمن قيام الحاسب الآلي بأداء المهمة المطلوبة بشكل صحيح وبالطريقة التي يرغبها المستخدم (غراب، وحجازي، ١٩٩٩م: ١١٩).

وتحتاج المؤسسة في نظام معلوماتها الإدارية إلى نظام تشغيل واحد وإلى العديد من البرامج التطبيقية لأداء المهام الإدارية والمحاسبية المختلفة. والطريقة الوحيدة للحصول على نظام التشغيل توفيره من الشركة الصانعة للتجهيزات الحاسبات الآلية أو من مؤسسات إنتاج البرمجيات، بينما يمكن الحصول على البرمجيات التطبيقية بطرق متعددة، منها التطوير الداخلي من قبل المبرمجين في المؤسسة أو التطوير من خلال التعاقد مع مؤسسات إنتاج البرمجيات أو من خلال شراء برامج تطبيقية جاهزة (برهان، ورحّو، ١٩٩٨م: ٧١).

ويتم اختيار الطريقة المناسبة للحصول على البرمجيات التطبيقية المطلوبة في ضوء عدة عوامل كتوفر مبرمجين يعملون ضمن المؤسسة، وإمكانية قيام المبرمجين بتطوير البرنامج المطلوب ضمن الحدود المناسبة من حيث التكلفة والزمن، وتوفر برامج جاهزة عند الجهات المتخصصة بالتوفير البرامج التطبيقية الجاهزة Software Packages والمصممة خصيصاً لأداء مهمة محددة، مثلاً إعداد حسابات، أو جداول الرواتب والأجور، أو إعداد الميزانيات، أو غير ذلك من العمليات ذات الطبيعة العامة والتي يمكن أن توجد في جميع المتطلبات. كما أن الحصول على هذه البرمجيات حق استخدام License For Use فقط لهذه البرمجيات، فملكيتها تبقى للمؤسسات المنتجة لها (برهان، ورحّو، ١٩٩٨م: ٧٤).

٢-٤-٣ قواعد البيانات

يعتمد نجاح نظم المعلومات على الإدارة الجيدة للبيانات، فدون ذلك لا يمكن ضمان دقة واكتمالية وموثوقية البيانات وبالتالي المعلومات الناتجة عن معالجة هذه البيانات. ومن هذا المنطلق

يهتم المختصون في مجال نظم المعلومات بقواعد البيانات Data Bases (برهان، ورحّو، ١٩٩٨م: ٧٧).

١. أهميتها

يتزايد الاهتمام بقواعد البيانات Data Bases نظراً لتزايد حجم البيانات المطلوب تخزينها واسترجاعها ومعالجتها في المؤسسة، مما يتطلب طرقاً وأساليب أكثر تطوراً وحداثة للتعامل مع هذا الحجم الكبيرة من البيانات. وتزايد الاهتمام بالبيانات واعتبارها مورداً قيماً Viable Resource من موارد المؤسسة، مما يتطلب العمل على إدارة هذا المورد بطريقة فعالة، كما ازدادت حاجة مؤسسات الأعمال إلى البيانات الدقيقة وذات الموثوقية العالية لاستخدامها في التخطيط والرقابة واتخاذ القرارات. وقد أصبحت المعلومات مفتاحاً لنجاح مؤسسات الأعمال وسر قوتها التنافسية (الشدي، ١٤٢١هـ: ٨٠).

٢. أهدافها

يهدف تخزين البيانات وتنظيمها ضمن قاعدة البيانات إلى تمثيل العلاقات المهمة والمتبادلة في عمل المؤسسة والتي يصعب تمثيلها باستخدام الملفات. وتنظيم البيانات بشكل قاعدة بيانات يساعد في ربط وتكامل وسلامة البيانات التي تهم المؤسسة. كما تهدف إلى تسهيل عمليات التخزين واسترجاع البيانات وتعديلها بمرونة كبيرة بالمقارنة مع أسلوب الملفات، حيث لا يمكن القيام إلا بعمليات محدودة. وتهدف أيضاً إلى ربط العلاقات الملفات وخصوصاً الملفات متغيرة البيانات، ببناء هيكل مناسب لتخزين البيانات والربط بينها من خلال العلاقات المنطقية لهذه البيانات (داود، أ، ٢٠٠٠م: ١٥٤).

٣. إدارتها

تتم إدارة قواعد البيانات Data Base Management باستخدام برمجيات خاصة تسمى نظم إدارة قواعد البيانات Data Base Management Systems. ويمكن بواسطة هذه البرامج إنشاء واستخدام وصيانة قواعد البيانات. ولأن النظم مستقلة عن التطبيقات فإنه يمكن استخدامها في جميع

أنواع التطبيقات. وتوفر نظم إدارة قواعد البيانات إمكانات وهي؛ إنشاء قواعد البيانات Data Base Creation بواسطة مدير قاعدة البيانات Data Base Administrator، وذلك على ضوء الهيكلية المعتمدة للبيانات المكونة للقاعدة. كما توفر تعريف هياكل البيانات Data Structures التي تسمح بالوصول إلى البيانات الموجودة في القاعدة دون معرفة كيفية تخزين هذه البيانات (برهان، ورحّو، ١٩٩٨م: ٨١).

كما تعرف البيانات Data Definition، وتحدد بنية لتخزينها Storage Structures Definition حيث يمكن تخزين بيانات القاعدة وفق بنى تخزينية Storage Structures متنوعة. ويقوم مدير قاعدة البيانات باختبار البنية التخزينية المناسبة في ضوء الطريقة التي ستستخدم فيها البيانات في التطبيقات المختلفة. وتوفر إدارة قاعدة البيانات الاستخلاص والاسترجاع Interrogation كعرض نتائج المعالجة على الشاشة أو طباعتها على الطابعة، كما توفر التحديث Updating والذي يتيح إضافة بيانات جديدة إلى قاعدة البيانات الموجودة فيها أو حذف البيانات غير الضرورية (برهان، ورحّو، ١٩٩٨م: ٨١).

٤-٤-٢

شبكات الاتصالات

١-٤-٤-٢ أهميتها في إدارة المؤسسات

تمكن الشبكات من التشارك في الموارد كالطابعات، والتطبيقات والبرامج، وقاعدة البيانات، بين العديد من المستخدمين مما يقلل من التكلفة، ويسهل عملية التحديث باستخدام نسخة واحدة يستخدمها الجميع، كما تقلل من الآثار المترتبة على الأعطال بسبب تعدد المسارات، وهذا يعتمد على نوع الشبكة المستخدمة. كما تسهل من إدخال العناصر الجديدة على الشبكة، وتنقل البيانات من جهاز إلى أخر بكمية كبيرة وسرعة هائلة، وعمل نسخ احتياطي عن طريق مدير الشبكة. وتعزز الشبكات من

قدرة الأمن، بحيث تجعل الحاسب الرئيسي مخزناً للبيانات وبقية الحاسبات الآلية مجرد نهايات طرفية (داود، أ، ٢٠٠٠م: ١٨٦).

٢-٤-٤-٢ مكوناتها

١. النهاية الطرفية Terminal: "يستطيع المستفيد الدخول من خلالها إلى الشبكة والاستفادة من خدماتها" (داود، أ، ٢٠٠٠م: ١٨٩). أو "أي جهاز إدخال أو إخراج يستخدم شبكة الاتصالات لإرسال واستقبال البيانات تعد محطة طرفية" (برهان، الرحو، ١٤١٨هـ: ١٤٢).

٢. قنوات الاتصال Channels: هي الوسائط التي يتم من خلالها انتقال البيانات من وسيلة الإرسال إلى وسيلة الاستقبال في شبكة الاتصالات كالأسلاك الملتوية Twisted Pair والأسلاك المحورية Coaxial Cable والألياف البصرية Fiber Optic وموجات الميكروويف Microwaves والأقمار الاصطناعية Satellites (المجلة الإلكترونية، ١٤٢٣هـ).

٣. معالج الاتصال Communication processor: "حاسب صغير يؤدي بعض وظائف الحاسب الكبير مثل تطبيق البرتوكول، واكتشاف الأخطاء وتصحيحها (داود، أ، ٢٠٠٠م: ١٩٠). ويقوم بتنظيم عملية إرسال البيانات بين المحطات الطرفية والحاسب الآلي.

٢-٤-٤-٣ انتقال البيانات من خلالها

يتم مرور البيانات من جهاز إلى أخر عبر خط رئيسي وخطوط فرعية بنفس الأسلوب، حيث تقسم البيانات إلى أجزاء صغيرة و ترسل على دفعات متتالية، وذلك لضمان وصول أكبر عدد من الدفعات بشكل سليم. وإذا حدث خطأ ولم تصل دفعه ما يقوم الجهاز المرسل بإرسال هذه الدفعة فقط وليس كامل البيانات. ويتم الإرسال بواسطة كروت الشبكة الموجودة على كل الأجهزة، إذ تقوم هذه الكروت بتحويل الإرسال المتوازي القادم من الجهاز المرسل إلى إرسال تسلسلي أو العكس، وتقوم

الكروت بعنونة الرزم بالعنوان المطلوب، ونقل الرزم إلى الشبكة، وتنظيم حجم وسرعة الإرسال، وعزل معلومات العنونة والمعادلة الرياضية لتصفية البيانات الحقيقية فقط (يونس، ١٩٩٤م: ٢٤٣).

٢-٤-٤-٤ البرتوكولات العاملة فيها

كي تتمكَّن الأجهزة الموجودة في الشبكة من تبادُل المعلومات فيما بينها، لا بد لها من مجموعة من قواعد الاتصال المعيارية المتفَّق عليها مُسبَقاً، وتدعى هذه القواعد بروتوكولاً Protocol. البروتوكولات، وهي اللغات التي تتخاطب بها أجهزة الحاسبات الآلية المتصلة عبر الشبكة، بهدف تبادل المعلومات، وهو وصف رسمي لهيئات الرسائل والقواعد التي يجب على جهازين إتباعها لتبادل تلك الرسائل (إنترنت العالم العربي، ١٤٢٣هـ).

٢-٤-٤-٥ معاييرها وطبقاتها

عندما يقوم مصممو برامج الشبكة بتصميم منتجاتهم يتبعون معايير وقواعد، وأكثر هذه القواعد انتشاراً هي مجموعة من التوصيات المطورة من قبل المؤسسة الدولية للمعايير ISO، وتعرف هذه التوصيات باسم النموذج المرجعي لنظام الوصلات المفتوحة OSI. لقد تم بناء نموذج OSI من سبع طبقات بروتوكول كل طبقة مسؤولة عن عمل ما تساعد على تحضير المعلومات من أجل الإرسال وتتفاعل كل طبقة مع الطبقات القريبة والمباشرة لها، إذ تعرض الطبقة خدمتها إلى الطبقة الموجودة فوقها وتطلب الخدمة من الطبقة التي تحتها (يونس، ١٩٩٤م: ٢٤٧).

تقدم كل طبقة خدمة معينة، فطبقة Application تزود برامج الشبكة مثل قواعد البيانات و البريد الإلكتروني بإمكانية الوصول إلى الشبكة والتي تتعامل مع Directory Services وActive Directory. وينحصر العمل الأساسي لطبقة Presentation بالتأكد من أن المعلومات المرسلة في الشبكة تستخدم نفس ترميز الأبجدية وتقوم أيضا بتشفير البيانات وضغطها، وأما طبقة Session فتشبه عمل السكرتير إذا طلب منه المدير أن يقوم بالاتصال بأحد الأشخاص فإن وجده حول له الخط، فهذه الطبقة تقوم

بنفس العمل، إذ تأسس الاتصال بين حاسبين وتقوم بمراقبة هذه الاتصال وكمية البيانات المرسلة وأحيانا تقوم بالتحقق من كلمات المرور عند إنشاء الاتصال (Nor٢٠٠٠, ٢٠٠٢).

وتنقل طبقة Transport البيانات وتكون مسؤولة عن تسليمها بشكل سليم من الأخطاء، وتقوم بتقسيم المعلومات إلى أجزاء صغيرة، وهي أيضا التي تقوم بالتجميع في الجهاز المستقبل، وتكون مسؤولة عن إشعار الاستلام من الحاسب المستقبل بأنه تم الاستلام بدون أخطاء. وتقوم طبقة Network باختيار أفضل الطرق التي يتوجه منها الإرسال وذلك حسب حركة المرور في الشبكة Traffic Load وتقوم أيضا بتوجيه إلى العنوان الصحيح إذ يوجد فيها بروتوكول (IP). وتنسق طبقة Data Link الرزم المقدمة لطبقه Physical والتحكم في التدفق الحاصل للبيانات، وإعادة إرسال البيانات التي تتعرض لتلف، وتعد طبقة Physical المسؤولة عن تحويل البيانات القادمة من الحاسب على شكل متوازي إلى شكل تسلسلي وتضع هذه البيانات على وسط النقل وتشتمل هذه الطبقة على مجموعة من التوصيات المعتبرة في الأرقام و الحروف (Nor٢٠٠٠, ٢٠٠٢).

٢-٤-٤-٦ أنوا عها

١. شبكة المنطقة المحلية (Local Area Network) LAN

هي أبسط أنواع شبكات الحاسب الآلي، تتصل من خلال أسلاك خاصة، ففي الأساس تحتوي على بضع عشرات من الحاسبات الآلية، ومجموعة من الأجهزة العاملة على الشبكة مثل طابعة أو طابعتين وكذلك ماسح رسوم، وقد يكون هناك أجهزة إضافية أخرى للحفظ (داود، أ، ٢٠٠: ٢٣٨). وتسمح بالتشارك بالموارد كالأجهزة المتصلة معها مثل أجهزه الفاكس والطابعات والمودم، والملفات، وقواعد البيانات، والبرامج، وغيرها (مدينة الملك عبد العزيز للعلوم والتقنية، ١٤٢٣هـ).

ويمكن لشبكة المنطقة المحلية أن تقوم بتأدية أعمال مختلفة، ففيها يمكن أن يتم إرسال المعلومات من جهاز لآخر بدون الحاجة لنقل تلك المعلومات من أحد الأجهزة إلى قرص لين لتشغيله.

وبسبب الفائدة الكبيرة التي تعود على المؤسسات فقد اهتمت المؤسسات الصغيرة ومتوسطة الحجم بإدخال نظم شبكات الحاسب الآلي لديها، وهذا أدى بدوره، لقيام كثير من الجهات الصانعة لها بإنتاج خطوط متكاملة من هذه المنتجات التي وجهتها لاستخدام تلك المؤسسات الصغيرة والمتوسطة وفروع المؤسسات الكبيرة (مدينة الملك عبد العزيز للعلوم والتقنية، ١٤٢٣هـ).

٢. الشبكة الواسعة (Area Network) WAN

هي شبكة لِتبادُل المعلومات ضمن مساحة جغرافية واسعة قد تشمل عدة دول، وهي أكبر من الشبكة المحلية LAN، وقد تستخدِم خطوط الهاتف والأقمار الصناعية وغيرها من وسائط نقل البيانات. ويمكن أن تربط عدة شبكات محلية، وتتيح نقلا آمنا وسريعا للمعلومات بين العُقَد المختلفة، وتحقّق المؤسسات الكبيرة التي تنتشر فروعها في أرجاء العالم الاستفادة الكُبرى من الشبكات الواسعة، لأن هذه الشبكات تُتيح لها الاتصال مع موظفيها وزبائنها وشركائها عبر العالم (Itep, A, ٢٠٠٢).

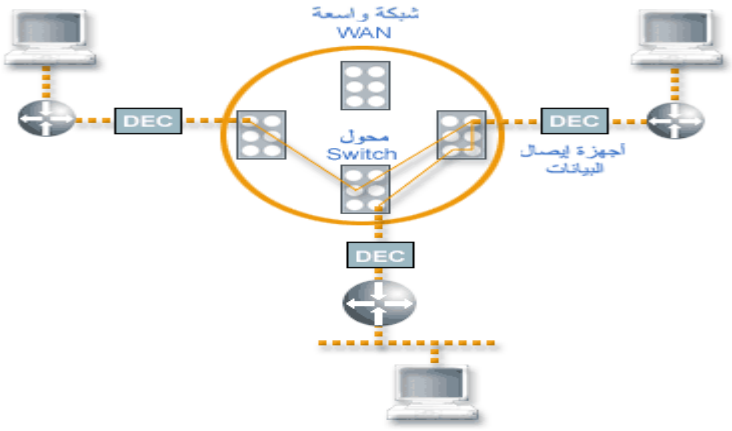
وللشبكات الواسعة دور كبير في تشجيع وحفز الأعمال الإلكترونية التي انتشرت في عصر الإنترنت، وفي أغلب الدول تقوم مؤسسات الاتصالات الحكومية (PTT) بالإشراف على الشبكات الواسعة وصيانتها كما تقدِّم هذه المؤسسات خدمات معيَّنة لمستخدِمي الشبكات الواسعة مثل خدمة الخط المستأجَر Leased Line. يتم توصيل الأجهزة ببعضها في الشبكات الواسعة بعدة طرق منها الوصل نقطة بنقطة Point-To-Point Connection وتعتمد هذه الطريقة الخطَّ المستأجر Line Leased لوصل مكانين متباعدين على الشبكة بوساطة وصلة وحيدة المصدر (Itep, A, ٢٠٠٢). وشكل رقم (٢) يوضح ذلك.

شكل رقم (٢) الوصل نقطة بنقطة في الشبكة الواسعة

المصدر (Itep, A, ٢٠٠٢).

ومنها أيضاً طريقة التحويل عبر دائرة Switching Circuit وتشبه طريقة إجراء المكالمة الهاتفية في شغلها لخط الهاتف أثناء فترة الاتصال. وتستخدم هذه الطريقة دائرة تُشكّل وصلة فعلية بين الأطراف المرسِلة والمُستقبلة عبر خط الهاتف، كما في شكل (٣). وأيضاً منها طريقة التحويل بالحزم Packet Switching وتعد الأساس لمعظم شبكات الاتصالات (Itep, A, ٢٠٠٢).

شكل رقم (٣) التحويل عبر دائرة



المصدر (Itep, A, ٢٠٠٢).

٣. شبكة الإنترانت Intranet

تطلق تسمية الإنترانت على التطبيق العملي لاستخدام تقنيات الإنترنت Web في الشبكة الداخلية للمؤسسة، بغرض رفع كفاءة العمل الإداري وتحسين آليات تشارك الموارد والمعلومات والاستفادة من التقنيات المشتركة. كما تقدم شبكة الإنترانت خدمة الدخول إلى الإنترنت. بحيث لا يمكن لغير المُسجلين في شبكة الإنترانت الدخول إليها عن طريق الإنترنت، وبذلك تؤمن الإنترانت سوراً منيعاً حول محتوياتها مع المحافظة على حق وصول العاملين عليها إلى مصادر المعلومات الخارجية على الإنترنت. يعمل جهاز الخادم Server في شبكة الإنترانت على تقليل الحاجة إلى وجود نسخ متعددة

من البرامج وقواعد البيانات Databases، لأن هيكلية موقع شبكة الإنترانيت مطابقة تماما لبنيته على الإنترنت، وتسمح هذه البنية بخدمة تنزيل الملفات والتطبيقات بسهولة ويسر (Itep, B, ٢٠٠٢).

كما إن الوصول إلى البيانات المشتركة يمكن أن يُنفذ عن طريق قاعدة بيانات مشتركة يتم الوصول إليها من المستخدمين كل تبعاً للصلاحية Permission الممنوحة له، كما يمكن للشركة أن تستغني عن الكثير من المطبوعات والنماذج الورقية التي تقدم الإنترانت حلولاً إلكترونية لها كدليل الهاتف Phonebook وطلبات الصيانة Maintenance Request Form والخدمات الإدارية المتعددة. إلى جانب ذلك يمكن اعتماد أجهزة متواضعة الإمكانيات للموظفين لأن الجهاز الخادم هو الذي سيقوم بجميع مهام التخزين وإدارة العمليات بواسطة الموقع الداخلي Internal Web Site وسيكون برنامج استعراض الإنترانت هو البرنامج الرئيسي، وقد يكون الوحيد، الذي يحتاجه الموظف لتأدية وظيفته. وتقدم شبكة الإنترانيت خدمات كالبريد الإلكتروني E-mail وتقنية الملفات الإلكترونية المحمولة Portable Electronic Documented وخدمة نقل الأخبار News Network وخدمة مؤتمرات الفيديو Conference Video (Itep, B, ٢٠٠٢).

٤. شبكة الإكسترانت Extranet

أنشئت شبكات الإكسترانت استجابة لما يتطلبه قطاع الأعمال من تشارك وتحالفات وما يقتضيه من أمن على المعلومات المتبادلة مع العناية الشديدة بالمصالح المشتركة عن طريق الشبكات. وشبكات الإكسترانت تعتمد على قطاع الأعمال الذي يُقسمها إلى أنواع منها شبكات إكسترانت التزويد Supplier Extranets التي تربط مستودعات البضائع الرئيسة مع المستودعات الفرعية بغرض تسيير العمل فيها آلياً للمحافظة على كمية ثابتة من البضائع في المستودعات وبالتالي تقليل احتمال رفض الطلبات بسبب وجود عجز في المستودع، إضافة للعديد من الخدمات الأخرى المتعلقة بالتحكم بالمخزون Inventory Point. ومن أنواعها شبكات إكسترانت التوزيع Distributor Extranets وتمنح هذه الشبكات صلاحيات للمتعاملين مُستندة إلى حجم تعاملاتهم، وتُقدم لهم خدمة الطلب الإلكتروني

وتسوية الحسابات آلياً، مع التزويد الدائم بقوائم المنتجات الجديدة والمواصفات التقنية وما إلى ذلك من خدمات أخرى. وشبكات إكسترانت التنافسية Peer Extranets تُعزز التنافس في القطاعات الصناعية، إذ تَمنح المؤسسات الكبيرة والصغيرة فرصة متكافئة في مجال البيع والشراء عن طريق ربط المؤسسات الصغيرة والكبيرة كي تنقل فيما بينها الأسعار والمواصفات التقنية الدقيقة مما يرفع من مستوى الخدمة في ذلك القطاع ويعزز جودة المنتجات ويقضي على الاحتكار (Itep, C, ٢٠٠٢).

٥. شبكة الإنترنت Internet

أ. **مميزاتها**: تتميز الإنترنت بكونها شبكة عالية وغنية، وسهلة، ويمكن النفاذ إليها في أي وقت، ومع انتشار الوصلات اللاسلكية في كافة المنازل والمكاتب والسيارات, ستصبح الإنترنت في كل مكان. كما ستصبح الإنترنت واجهة بينية طبيعية وبالتالي ستغدو الاجتماعات الإلكترونية على الإنترنت من الأمور الاعتيادية. وستصل إلى مستوى أعلى من وذلك من خلال دمج سلاسل التوريد والمعاملات التجارية بين المؤسسات، ولن يتم وصل المؤسسات بالعملاء فحسب, بل أيضاً بالموردين والشركاء مما يسمح بالتبليغ عن الموجودات وسد النقص في المخزون من الموردين بشكل تلقائي. وستدمج التطبيقات المختلفة بسهولة في الإنترنت بواسطة المعايير الموحدة والنظم المفتوحة والبرامج المتوافقة معها (Itep, D, ٢٠٠٢).

وتقدم الإنترنت خدمات كنشر الأبحاث وأوراق المحاضرات، والكتب والمراجع، والملخصات العلمية، وأدلة التقنية Technical Manuals بصيغة يمكن استقبالها وقراءتها عبر شبكة الإنترنت. وتتميز تلك الوسائط بأنها صيغة مضغوطة Compacted ومدعومة بوسائط وأدوات كالأصوات والرسوم ونقاط التوصيل Hyperlinks التي تربط القارئ بمعلومات فرعية أو بمواقع على شبكة الإنترنت. وهناك عدد من هيئات النشر على صفحات على الإنترنت من أهمها؛ HTML (Hypertext Markup Language)، Post Script، Acrobat PDF (Portable Document Forma) (موسوعة الكمبيوتر والإنترنت، ٢٠٠٢م). كما تقدم الإنترنت خدمات أخرى كالأعمال المصرفية

التي تتم من خلالها، ونقل الملفات (File Transfer Protocol) FTP، والمحادثات الفورية، والاتصال من بعد Telnet (Itep, E, ٢٠٠٢). ومجموعات الأخبار Newsgroup، والحكومة الإلكترونية. كما نعتبر الإنترنت وسيلة تحرٍ للأجهزة الأمنية عن الجرائم، والتدريب والتعليم، والقيام بأعمال التجارة الإلكترونية (بحر، ١٤٢٠هـ: ٢٨).

ب. **مستقبلها**: بدأ الجيل الثاني من الإنترنت بالظهور على أرض الواقع، ويتمثل ذلك في عدة مشاريع منها Internet٢، وإنترنت الجيل المُقبل (Next Generation Internet) NGI، وشبكة Canet٢. ويعتمد هذا الجيل نسخة مطوَّرة من بروتوكول الإنترنت، هي IPv٦ كما يدعم ميزتين مهمتين هما: الإرسال المتزامن المتعدد الوجهات Multicasting، وميزة جودة الخدمات Quality Of Service-Quos بهدف دعم البث الحي لملفات الفيديو، وتطبيقات الوسائط المتعددة Multimedia. وما زال الجيل الثالث للإنترنت قيْد الأبحاث، ومن المتوقَّع له أن يدعم جميع المزايا المتقدمة، ولا سيَّما تلك التي تتطلَّب سرعة عالية جداً، ومن أبرز المشاريع المقدَّمة شبكة Canet٣، وشبكة Super Net. ويدعم هذا الجيل ميزتين مهمَّتين هما؛ استخدام تقنية DWDM (Dense Wavelength Division Multiplexing)، وهي تقنية تستخدم الألياف الضوئية في الإرسال بسُرعات تصل إلى (٤٠٠) غيغابت/ثانية، مما يسرِّع نقل الصوت والفيديو بدرجة هائلة، واستغلال الألياف المعتِمة Dark Fiber في التحويل Switching والتوجيه (Itep, A, Routing ٢٠٠٢)

وسيؤدي هذا التطور إلى ثورة في مجال التجارة الإلكترونية، وسيساعد على طرح العديد من الأجهزة القادرة على الدخول إلى خدمات الإنترنت، كما أن هذا التطور سيؤدي إلى انتشار تطبيقات على الإنترنت كالتلفزيون التفاعلي Interactive TV، والتعليم الإلكتروني E-Learning، ومؤتمرات الفيديو Video Conferencing. وأما تطبيقات الواقع الافتراضي Virtual Reality، فستمكن العلماء من أن يتشاركوا عن بُعد بأجهزة ذات تقنية عالية مثل الميكروسكوب، وسيتمكن

الأطباء من معاينة مرضاهم وإجراء العمليات الجراحية لهم باستخدام إنترنت الجيل الثاني Virtual Surgery، إضافة إلى ظهور المتاحف والمكتبات الافتراضيVirtual Libraries And Museums (Itep, A, ٢٠٠٢).

ج. **طرق الاتصال بها**: توجد عدة طرق للاتصال بالإنترنت، كالاتصال الشبكي الهاتفي Dial-up مع موفّر خدمة الإنترنت (Internet Service Provider) ISP، وهذه هي الطريقة المعتادة لدى مستخدمي أجهزة الحاسب الآلي في المنزل، وعن طريق الخط المُخصَّص Dedicated Line المتصل بشبكة محلية LAN، وتكون متصِّلة بموفّر خدمة الإنترنت ISP، أو قد يكون لها عُقدة Node خاصة بها على الإنترنت، وهذه هي الطريقة المعتادة لدى المؤسسات الكبيرة. كما يمكن أن يتم الاتصال بشبكة الإنترنت عبر الأقمار الاصطناعية (Itep, D, ٢٠٠٢)

٢-٤-٥ الأفراد

تحتاج المؤسسات إلى عدة تخصصات يشغلها مجموعة من الأفراد المتخصصين في مجال الحاسب الآلي والشبكات. فمدير قاعدة بيانات يكون اختصاصه بناء قاعدة بيانات للنظام المعلوماتي، كما يتأكد من عمل نظام قاعدة البيانات بالشكل المطلوب، كما يقوم محلل النظم بدراسة وتصميم نظم المعلومات المطلوبة والمساعدة في بناء نظم المعلومات، كما يتعاون مع المبرمج والمستخدمين في بناء نظم المعلومات، ويكون تصميم البرامج وتطوير البرامج الجاهزة من اختصاص المبرمج. وعندما تريد المؤسسة بناء شبكاتها فتعهد لمهندس الشبكات بدراسة وتصميم وتطوير شبكة الاتصالات والإشراف على تمديد الشبكات وإدارة الأجهزة المركزية للشبكة وإدارة خدمات الشبكة، ويساعده في مهامه فني الشبكات والمسؤول عن تركيب وإعداد وصيانة معدات ونظم الشبكة ويكون من ضمن اختصاص مدير النظام System Administrator إعداد مصادر الشبكة وتسجيل المستخدمين وأرقامهم السرية وصيانة المصادر (Iugaza, ٢٠٠٢).

وعند إنشاء موقع للمؤسسة فإن مسئول الموقع Web Master يكون من اختصاصه مراقبة الموقع، وتحديثه، والأشراف عليه، وإذا أرادت المؤسسة المحافظة على معلوماتها فيترتب عليها إنشاء قسم يرأسه مدير أمن النظام، ويعمل معه مدققون Auditors، وأخصائيو حلول أمن المعلومات، وأخصائيو النظام، ومراقبة الشبكات، وقد يكون أكثر العاملين في المؤسسات هم مدخلو البيانات، ومستخدمو الحاسب الآلي Users، والذين لا يحتاجون إلى تلك المهارة الفنية بل يتعاملون مع نهاية طرفية. ويتطلب قسم الصيانة فني صيانة حاسب يقوم بإصلاح أعطال الحاسبات الآلية والتجهيزات الملحقة بها، ويقوم بصيانة وتحديث البرامج في الحاسبات الآلية والتجهيزات الملحقة بها.

٢-٥ خلاصة الفصل الثاني

تم تناول المعلومات وذلك بالتطرق إلى أهميتها، وحرب المعلومات، وتوضيح مفهوم المجتمع المعلوماتي، كما تم تناول نماذج نظم المعلومات والتي منها نظم المعلومات الإدارية، ونظم معالجة العمليات، ونظم المعلومات الصحية، ونظم المعلومات الجغرافية، والنظم الخبيرة. أما مكونات النظام فشملت الحاسبات الآلية، والبرامج، وقواعد البيانات، والشبكات، والأفراد المتخصصين في جميع أجزاء النظام، وقد أوضح الباحث دور كلٍ من هذه المكونات بصورة مختصرة.

الفصل الثالث/ التحقيق في جرائم نظم المعلومات

٣-١ المقدمة

يتطلب التحقيق في جرائم نظم المعلومات الاطلاع على الإجراءات الأمنية المتبعة في حماية النظام المعلوماتي، والسياسات الأمنية المعمول بها، ومعرفة الإجراء المتبع بعنصر النظام ذي العلاقة بالجريمة كخطة تأمين قاعدة البيانات، والشبكات، والأجهزة وغيرها. في هذا الفصل يستعرض الباحث أنماط جرائم نظم المعلومات وأساليب وأدوات ارتكابها، وخصائصها، وأصناف مجرميها، وأسباب انتشارها، ودوافعها. كما ستناول الباحث وسائل التحقيق والعوائق التي تحول دون استخدام تلك الوسائل وأخيراً يتم التطرق إلى الأدلة المثبتة.

٣-٢ أمن نظم المعلومات

أصبح أمن نظم المعلومات من أهم الأوليات التي تحرص عليها المؤسسات المختلفة، فالاعتماد على نظم المعلومات يزداد بصورة متسارعة، يقابله على الاتجاه الآخر زيادة في المخاطر التي قد تتسبب في تهديد تلك النظم. ومع وجود الإنترنت وارتباط الكثير من الجهات بها، زادت التهديدات بشكل كبير، ولم تعد حماية المعلومات روتينية أو سهلة بالقدر الذي كانت عليه في الماضي، مما زاد من أهمية أمن المعلومات كعملية متكاملة مستمرة في مسيرة نظام المعلومات، وأصبح التخطيط لها علماً مستقلاً يحرص على الموائمة بين احتياجات الجهة ومتطلبات أمن المعلومات (العِلم لأمن المعلومات، ١٤٢٣هـ). ويتركز أمن المعلومات حول أمن ووحدة وسرية وجاهزية المعلومات والمعدات، والأجهزة، وملحقاتها، والبرمجيات والمواد المستهلكة، وخدمات الحاسب الآلي. كما يتركز حول تحديد الأخطار التي تواجه نظم المؤسسة وعملية مواجهتها والسلامة من الكوارث وأمن وحماية

الحاسبات الآلية وأمن الأفراد (لجنة المعايير، ١٩٩٤م). هناك مجموعة من التحديات التي يجب أخذها في الحسبان لضمان نقل المعلومات عند استخدام النظم، ويمكن حصرها في أربعة محاور، على النحو التالي:

١. **خصوصية المعلومات Privacy**: وتعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين بذلك (الهاجري، ١٤٢٢هـ). ولكي تتم المحافظة على خصوصية المعلومات، يجب ألا يتمكَّن من الاطلاع عليها إلا الأطراف المعنية المسموح لها بذلك (مدينة الملك عبد العزيز للعلوم والتقنية، ١٤٢٣هـ).

٢. **سلامة المعلومات Integrity**: ويتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين بذلك (الهاجري، ١٤٢٢هـ)، وذلك لمنع أي تغيير للمحتوى بشكل متعمَّد أو غير مُتعمَّد، وتكمن أهمية ذلك في الحفاظ على محتوى مفيد وموثوق به. وفي الغالب تكون الأخطاء البشرية وعمليات العبث المقصود، هي السبب في تلف أو تشويه البيانات، وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام (مدينة الملك عبد العزيز للعلوم والتقنية، ١٤٢٣هـ).

٣. **التحقق من هوية الأطراف الأخرى Peer Authentication**: إذ يجب على كل طرف معرفة هوية الطرف الآخر لتجنب أي شكل من أشكال الخداع، مثل عمليات التزوير وانتحال الشخصيات (مدينة الملك عبد العزيز للعلوم والتقنية، ١٤٢٣هـ).

٤. **توفر المعلومات Availability**: ويتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسب إلا من قبل الأشخاص المخولين بذلك (الهاجري، ١٤٢٢هـ). كما لا بد من توافر البيانات المطلوبة للمستفيد عند طلبها (داود، أ، ٢٠٠٠: ٢٣٢).

٣-٢-١ الإجراءات الإدارية لأمن المعلومات

على الإدارة العليا القيام بعدة مهام تجاه أمن المعلومات كالرقابة الإشراف على أمن المعلومات، وسوف يتم استعراض مهام رئيسة يجب عليها القيام بها، وهي كالتالي:

٣-٢-١-١ توفير أمن الأجهزة

لتأمين الأجهزة لابد من تأمين المبنى كعدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين (داود، أ، ٢٠٠٠م: ٢٢٦). ويفضل استخدام التقنية للدخول على الأنظمة (بصمة الإصبع، بصمة العين، البطاقة الممغنطة .....الخ). كما ينبغي إعداد خطة طوارئ تتبع في حالة حدوث كوارث طبيعية، أو صناعية (عبد المطلب، ١٤٢٠هـ: ١٢١). ومن الضروري تأمين الخدمات التي قد يسبب توقفها تلفاً بالأجهزة، مثل الطاقة الكهربية، والتكييف، وتأمين النهايات الطرفية والطابعات، ومراقبة أماكن الطباعة التي يتم فيها إخراج النسخ المطبوعة لتقليل فرصة الحصول على قوائم بيانات مطبوعة، وإغلاق طرق الوصول إلى الطرفيات (داود، أ، ٢٠٠٠م).

٣-٢-١-٢ توفير أمن البيانات

يتوجب على الإدارة توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني، وتقليص الجرائم، ووضع آلية يتم تنفيذها للقيام بالنسخ الاحتياطي وتأمين وسائط الحفظ الخارجية بما يكفل أمنها وتحديثها، ويجب صياغة الضوابط المنظمة لعمليات التشغيل، ولمبرمجي قواعد البيانات ومدرائها، ولإدارة الشبكات وخطوط الاتصال، ولعمليات الإدخال والإخراج، والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية (الشدي، ١٤٢١هـ). ومن الأفضل في أغلب الأحوال توفير أجهزة بدون محركات أقراص لعدم إتاحة استخدامها، كما يجب رصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم بواسطتها، واستخدام وسائل حماية تساعد في تتبع المجرمين، والتأكد من مزامنة ساعات الأجهزة باستمرار، وذلك لأنه يساعد في تحديد وقت وقوع الجريمة. ولا

بد من وضع إجراءات تطبق في حالة وقوع جريمة كتشكيل فريق طوارئ للتعامل معها. كما يجب على الإدارة وضع ضوابط لأعمال صيانة الأجهزة، وتحديث البرامج، وتحديد جميع الإجراءات الأمنية لحماية بياناتها (داود، أ، ٢٠٠٠م).

٣-٢-١-٣ توفير أمن الأفراد

عندما تريد الإدارة حماية معلوماتها عليها إتباع الإجراءات الإدارية في مجال أمن الأفراد على النحو التالي (الشدي، ١٤٢١هـ: ١٨٥):

١. إخضاع الموظفين الذين سوف يعملون في مناطق حساسة للتحريات الأمنية للتأكد من سجلهم الجنائي قبل قبولهم في تلك الوظائف الحساسة.

٢. إطلاع الأفراد على السياسة الأمنية وتوقيعهم عليها، ومعاقبة المخالفين لتعليماتها بالعقوبات المناسبة.

٣. منع التوظيف المؤقت نهائياً، ومراعاة إجراءات إنهاء خدمة الموظف بطلب تسليم كل ما كان بحوزته كالمفاتيح والبطاقات الممغنطة، وتغيير كلمة المرور قبل مغادرته.

٤. متابعة العاملين ونقلهم إجبارياً بين الأقسام المختلفة في الإدارة، وملاحظة الذين لا يطلبون إجهازه بإجبارهم على الإجازة ومراقبة النظام بعد ذلك للتأكد من عدم وجود خلل كانوا يتفادونه بوجودهم.

٥. عقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال أمن المعلومات، والاشتراك في المجلات المتخصصة بأمن المعلومات، وعرض النشرات الداخلية وتعليمات الإدارة Memo التي تتضمن إطلاع الأفراد على المعلومات المهمة في مجال الأمن، لإلزام العاملين بالنظم الإدارية المحددة.

٦. ندب العاملين لحضور المعارض العالمية للأجهزة والبرامج، والإبتعاث إلى الدورات المتخصصة بأمن المعلومات، ليكون لديهم خلفية قوية بما يكفل تحقيق أمن المعلومات بالمؤسسة.

٧. لابد من اعتماد تجزئة الأعمال والمهام الحساسة وعدم احتكارها من البداية إلى النهاية لدى شخص معين.

٨. منح الحوافز وربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات.

٣-٢-١-٤ القيام بالتدقيق الأمني

يعطي التدقيق الأمني للبنية التحتية لتقنية المعلومات من منظور (داخلي/ خارجي) وفق معايير (BS٧٧٩٩) ومعايير (ISO١٧٧٩٩) صورة جيدة للوضع الأمني القائم بالمؤسسة، كما يساعد صناع القرار ومدراء تقنية المعلومات على الإطلاع الشامل على أمن بيئة تقنية المعلومات لمؤسستهم. معرفة مدى صحة إتباع الإجراءات والقوانين والنظم الداخلية وكذلك الخطوات الفنية الخاصة بحماية المعلومات في المؤسسة بصورة سليمة ليست بالمهمة اليسيرة ولكن التدقيق الأمني يجعل من تلك المهمة أمراً في غاية السهولة. وخلال عملية التدقيق الأمني تتم مراجعة إجراءات حماية تقنية المعلومات في المؤسسة ومعرفة مدى مطابقتها للاحتياجات، ومن ثم التحقق من تدوين أي محاولات لانتهاك تلك الإجراءات (Comguard, ٢٠٠٢).

وبتجميع شواهد متعددة وشاملة حول العمليات التي تمت في نظام المعلومات يتم اكتشاف أي محاولة للإخلال بأمن المعلومات، وكذلك نقاط الضعف في بنية النظام والتي تسببت في تلك المحاولات. ويتم مراجعة الخطط الخاصة بالطوارئ وإدارة الأخطار لتحديد مدى ملاءمتها ومدى الحاجة لمراجعتها (العِلم لأمن المعلومات، ١٤٢٣هـ). ويشمل التدقيق الأمني الكشف عن مدى مراعاة الجانب الأمني في خطة استمرارية العمل، وطريقة التحكم بالنفاذ إلى نظم إدارة أجهزة

الحاسب الآلي والشبكات، وإجراءات صيانة أجزاء النظم، وأمن البيئة وأعمال الحراسة الأمنية، وتحديد الموارد والتحكم بها، وأسلوب تحقيق الأمن الشخصي (Comguard, ٢٠٠٢).

٣-٢-١-٥ توفير قسم متخصص بأمن المعلومات

تقوم المؤسسات الكبيرة بتعيين مدير أمن لنظم المعلومات يرتبط بالإدارة العليا مباشرة لأهمية التقارير التي يعدها. ويرأس مدير أمن هذا قسماً مستقلاً من المتخصصين في مجال أمن المعلومات ومن ذوي الخبرة الفنية والأمنية في معالجة البيانات والبرمجة حسب نظم التشغيل ولغات البرمجة وقواعد البيانات المستخدمة في المؤسسة، محددة تخصصاتهم حسب مسؤولياتهم في القسم، ومدربين على التنسيق الأمني ولديهم المقدرة الكافية للتعامل مع جرائم نظم المعلومات والحالات الطارئة (الشدي، ١٤٢١هـ: ١٥٣). ويشرف مدير أمن المعلومات على إجراءات الأمن بالمؤسسة، وينسق مع فريق تطوير النظم، ومداراء الشبكات، وفريق الصيانة، وعقود توريد الأجهزة والبرامج حتى يتأكد من مطابقتها للنواحي الأمنية، كما يشرف أيضاً على سير السياسة الأمنية بالمؤسسة، ويكون على إطلاع على كل ما هو جديد في مجال جرائم نظم المعلومات، وأمن المعلومات.

٣-٢-٢ الإجراءات الفنية لأمن المعلومات

٣-٢-٢-١ توفير الحماية الإلكترونية

تخضع الحماية الإلكترونية للإعدادات الخاصة بالحاسب الآلي، والأجهزة الملحقة به، ويمكن بيانها على النحو التالي (المجلة الإلكترونية، ١٤٢٣هـ):

١. حذف الملفات غير الهامة ولو كانت المعلومات التي تحويها ضئيلة وعديمة الفائدة، لأنها في المقابل قد تكون ثمينة بالنسبة للآخرين، وقد تكون الخيط الرفيع الذي سيقودهم إلى معلومات أكثر أهمية، فلابد من حذفها بشكل نهائي والتأكد من عدم إبقاءها في سلة المحذوفات Recycle Bin. وعملية حذف الملفات من القرص الصلب Hard Disk، لا تحذف المحتويات فعلياً، ولا يقوم نظام

التشغيل Operating System بمسحها من القرص الصلب، بل يقوم بتغيير الحرف الأول من ملف Table Root Directory، أي إزالة فهرس المسار فقط. أن مساحة هذا الملف يمكن استعمالها لملف آخر، وبشكل عرضي يتم كتابة بيانات الملفات الجديدة على هذه المساحات فوق البيانات القديمة، وإظهار البيانات القديمة كملف يمكن للحاسب الآلي والتطبيقات قراءته. ولاستعادة الملفات المحذوفة هناك برامج مثلWindows For File Rescue، Research Regnerud يمكنها البحث في Root Directory Table عن الملف الذي يراد استعادته ومن ثم استعادته. ولإزالة تلك البيانات القديمة يتم استخدام أدوات تقوم بحذف الملفات من المساحات حذفاً لا يمكن استعادته بعد ذلك، مثل Windows Wash Norton ٢٠٠٠, Utilities -Remove.

٢. حماية البيانات عند ترك الجهاز ولو لبضع دقائق، لأن الوصول للمعلومات يكون بدقائق معدودة، ويتم ذلك بإيقاف النظام بشكل مؤقت أو ما يعرف بعملية السبات حيث تطفي الشاشة فيبدو كأنه مغلق، وهذا يبعد أعين الفضوليين عنه، وفي حالة عدم توفر ميزة السبات فيمكن إطفاء الشاشة، أو نزع سلكها من الطاقة أو نزع سلك لوحة المفاتيح والفأرة.

٣. الكشف على الحاسب الآلي بعد الغياب عن طريق المستكشف، بإلقاء نظرة على زمن إنشاء الملف، ثم بإلقاء نظرة على زمن أخر تعديل وزمن أخر فتح للملف، فإن كان زمن وتاريخ أخر فتح للملف بعد أخر استخدام للحاسب فإنه تم استخدامه من قبل شخص آخر. وتركيب برامج تمنع مسح المعلومات من المستكشف، أو استخدام برامج تحتفظ بالعمليات التي تم إجراءها.

٤. مسح الآثار من قائمة المستندات، لأنها تبقى ركيزة أساسية للاختراق، ونسخ البيانات الحساسة على قرص مرن خارجي، وحذف الملفات الأصلية والهامة عن القرص الصلب، إلا أن تكون مورداً يخدم أكثر من مستفيد، وعدم ترك الملفات المهمة بالقرص الصلب وخصوصاً عند الارتباط بالشبكات.

٥. أخذ الاحتياطات الأمنية المتعلقة بتغيير الإعدادات للتطبيقات ولنظام التشغيل كإخفاء شريط المهام، حتى لا يتمكن قليل الخبرة من معرفة مكانه، بجعله على وضع الإخفاء التلقائي Auto Hide لشريط المهام، ليخفي قائمة " إبداء" وأسماء البرامج، ومنع تعديل الملف من قبل الآخرين عن طريق الخطأ أو العمد وجعله للقراءة فقط Read Only.

٦. استخدام كلمات المرور في Windows، مع أنه يوفر كلمات مرور خاصة لحماية نظام التشغيل، إلا أن هذه الحماية تفتقر للقوة اللازمة لأن كسرها سهل للخبير، أما المستخدم العادي فبإمكانه تعلم تجاوز هذه الحماية من خلال ملف التعليمات Help الملحق في Windows. وهناك أنواع من كلمات المرور التي يستطيع المستخدم استخدامها مثل كلمة المرور لشاشة التوقف، وكلمة المرور الخاصة بالشبكات، وكلمة المرور لتشغيل الحاسب الآلي مع أن كلمة المرور من هذا النوع تكون حاجزاً إلا أنها في نفس الوقت تتسم بالضعف، لأنها تستمد طاقتها من BIOS الذي يحتفظ بها مستعينا ببطارية الحاسب الآلي، فيمكن تجاوزها بفتح الجهاز وسحب البطارية الداخلية ثم إعادتها لمكانها، وأيضاً يمكن تجاوز كلمة المرور هذه بالاستعانة بقرص تشغيل النظام أو قرص DOS. ومنع استخدام الأمر Net Use لتعطيل خدماتNet Bios.

٧. استغلال برنامج WinZip كنظام حماية مرور Password لعدد كثير من الملفات المراد حمايتها. وضغط الملفات وحمايتها بكلمة مرور، ولكن الأفضل استخدام أحد البرامج الجيدة للحماية الأمنية بكلمات مرور قوية لا يمكن تجاوزها عن طريق التطبيقات الشائعة، والتي يمكن توفيرها من المصادر الموثوقة.

٨. إخفاء الملفات والمجلدات والتطبيقات والبرامج من على سطح المكتب ومن القرص الصلب بوضعها على وضع مخفي Hidden، حيث يمنع نظام التشغيل إظهار أسماء الملفات، بينما تكون هذه الملفات موجودة ويمكن للمستخدم أن يشغلها طالما أنه يعرف أسمائها.

٩. عدم استخدام الأسماء التي تجذب انتباه مخترقي أجهزة الحاسب الآلي سواء كان بالوصول المباشر أو عن طريق الشبكات كالملفات الشخصية، أو الصور الخاصة، أو الحسابات المصرفية، أو أرقام بطاقات الائتمان وغيرها، فمن الأسلم تسميتها بأسماء لا تلفت الانتباه كالحفظ باسم Calendar.Xls بدلاً من Budget.Xls، وتغيير إسم الملحق للملف لتعزيز الحماية القصوى، مع ملاحظة أنه إذا تم تغير إسم ملحق الملف قد يصعب استخدامه، وذلك بإخفاء ملف بوضعه في مكان لا يتوقعه أحد، فمثلاً وضع ملف Excel أو Word أو أي ملف مهم، بوضعه من ضمن مجلدWindows/System.

١٠. سد منافذ الاختراق. حينما يقوم المخترق بعملية المسح الشامل Port Scanning فإنه يبحث عن أمور مهمة في أجهزة الضحايا كالمنافذ المفتوحة Ports، أو الحصول على كلمة أو كلمات السر الخاصة بالضحية، وفي حالة الاتصال بالشبكات مع الإبقاء على تنشيط خاصية التشارك ودون استخدام تطبيقات تقوم بمراقبتها فإنه يمكن للمخترقين الدخول عبر منافذ التشارك في الموارد. وفي حالة التشارك يلزم استخدام تطبيقات تقوم بمراقبة منافذ التشارك في الموارد، ولسد ثغرة التشارك في الملفات والطباعة مع إبقائهما نشطتين في حالة الشبكات يجب استخدم جداراً نارياً مزوداً بخاصية سد تلك المنافذ مثل Black Ice Defender، أو حذف كلمات السر من PWL بواسطة برنامج WAPS٠٠٧.

١١. التأكد من عدم وجود برامج تجسس من فئة أحصنة طروادة في حالة الارتباط بشبكات في الحاسب الآلي حيث لا يرصدها برنامج الحماية لأنه تعد برتوكولات اتصال، وذلك بتشغيل برنامج الحماية بشكل دوري وتحديثه دائماً من مصدرة الأصلي.

١٢. أخذ الاحتياطات حول وWindows والتطبيقات الأخرى التي تقوم بحفظ المستندات بشكل متتابع خوفاً من احتمال انهيار النظام، وبعض التطبيقات تحفظ النصوص المحذوفة والمنقولة والمنسوخة ضمن مستند يحفظ في ملفات القرص حتى لو لم يقام بحفظ الملف الذي يعمل عليه، ولذا يجب

مسح وحذف الملفات المؤقتة Temp الغير ضرورية والموجود في Windowstemp مع ملاحظة أن Windows يستند عليها في حفظ الملفات المؤقتة.

١٣. استخدام نسخة أصلية وحديثة من نظام التشغيل وذلك لأن نظام التشغيل هو أساس الحماية ولكنه يمكن أن يكون أكبر نقطه ضعف في جهاز الحاسب الآلي. وتقوم المؤسسات المنتجة لنظم التشغيل بتحديث وتعديل هذه النظم كلما تم اكتشاف خلل أمني.

١٤. عند استخدام الإنترنت يجب عدم حفظ كلمة المرور الخاصة بالمستخدم وقت الدخول للإنترنت، وغلق المتصفح حال الابتعاد عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح، وعدم استخدام خاصية تذكر أسم المستخدم، وكلمة العبور، وعدم استخدام خاصية الإكمال الآلي للاسم، وفراغات النماذج في المتصفح، وعدم استخدام خاصية تذكر الصفحات التي تتم زيارتها لفترات طويلة، وتقليل هذه المدة على قدر المستطاع. تعديل خاصية الأمن في المتصفح الخاص إلى المستوى المتوسط أو الأعلى مع تعطيل خاصية الجافا سكريبت، وتعديل مستوى الأمن في خاصية الأكتف إكس.

١٥. عند استخدام البريد الإلكتروني يجب عدم فتح الملفات المرفقة إلا بعد التأكد منها، وعدم تحويل الرسائل المشبوهة، وعند الانتهاء من قراءة الرسائل يجب عمل Sign out ومن ثم الخروج بطريقة صحيحة من الموقع أو البرنامج لأن هنالك بعض برامج البريد أو المواقع تتذكر الزائر لمدة تصل إلى (٨) ساعات.

١٦. من الضروري تركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز، إن هذا يتيح لهذه البرامج البحث عن الفيروسات وتدميرها سواء كان أسبوعياً أو يومياً أو عند التشغيل. ومن الضروري أيضاً تحديث برامج مستكشف الفيروسات بصورة دورية، من خلال الحصول عليها من الشركة المنتجة، أو من مواقع إنترنت المختلفة، لضمان الحصول على آخر المعلومات والأعراض الخاصة بالفيروسات الجديدة، وطريقة الوقاية منها.

١٧. تشغيل برامج مستكشف الفيروسات، وتفحّص أي ملفات أو برامج جديدة تصل عبر البريد الإلكتروني، والإنترنت، والأقراص المرنة. وعدم السماح بإدخال وتشغيل أي ملفات أو برامج مجهولة المصدر وبدون الفحص مسبقاً، والانتباه إلى عدم تشغيل أو إعادة تشغيل الحاسب الآلي بوجود القرص المرن في موقعه، حيث أن بعض هذه الفيروسات تختبئ داخل القرص المرن حتى تجد الفرصة الملائمة للتشغيل عندها.

٣-٢-٢-٢ تأمين جميع مكونات الشبكة

في حالة استخدام الشبكات، فإن الحماية في هذه الحالة تعتمد على التحقق من الشخصية، للدخول إلى الشبكة، وعلى وسائل أمن الشبكة والتي يجب فحصها بالكامل وتقييم إمكانية اختراق نظام الحماية وتحديد تلك المخاطر المتعلقة بالتصميم والإدارة. لذا فإنه يجب القيام باختبارات اختراق ويلزم إجراء اختبار مفتوح لكل أساليب الاختراق المعروفة باستعمال كافة المعلومات المتاحة عن النظام المعلوماتي وإمكاناته، والقيام بتقييم التوافق مع الإجراءات الأمنية وتصميم الشبكة (العِلم لأمن المعلومات، ١٤٢٣هـ).

ولحماية الشبكات يلزم استخدام برامج حماية، كبرنامج LookDown٢٠٠٠ الذي تنتجه Harbor Telco Security Corp وهو من اشهر البرامج المستخدمة للحماية، ويعمل كجدار ناري يقوم بفحص الجهاز عند بدء التشغيل للبحث عن أحصنة طروادة ومن ثم إلغاء الملف مباشرة مع ترك رسالة تعلم المستخدم بذلك كما يمنع كذلك المخترقين ويسجل محاولات الدخول في تقرير مختصر يشمل وقت الدخول وعنوان (IP) كما انه يعطي معلومات عن جهة الاتصال، من عيوبه أنها تنطلق صفارة التحذير عند كل تغيير يحدث بملف Registry وعند استقبال cookies غير مضرة للمواقع التي تتم زيارتها (Comguard, ٢٠٠٢). ويوجد عدد من برامج الحماية الأخرى مثل برنامج Jammer وبرنامج٩٩ Internet Alert، وبرنامج ٢٠٠٠ Norton Internet Security، وبرنامج Net Buster، وبرنامج Conceal، وبرنامج ٢,٥ Bulls Eye، وبرنامج Zone Alarm (الفنتوخ، ١٤٢١هـ: ٤٩).

٣-٢-٢-٣ استخدام التشفير

إرسال البيانات عبر الشبكات يجعل من السهل التنصت عليها، والطّريقة الوحيدة لمنع هذا التنصت هي استخدام التّشفير (Barman, ٢٠٠١). يُعرَّف التشفير Encryption بأنه عملية تحويل المعلومات إلى شفرات غير مفهومة تبدو غير ذات معنى لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة. وتشكّل الإنترنت الوسط الأضخم لنقل المعلومات الحساسة، فإن أُريدَ الحفاظ على سلامتها وتأمينها فلابد من تشفيرها (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

كانت بداية استخدام الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب، خوفاً من وقوع الرسائل الحساسة في أيدي العدو، وقام يوليوس قيصر بتطوير خوارزميته المعيارية المعروفة باسم شفرة قيصر Caesar Cipher التي كانت نصّا مشفَّراً لتأمين اتصالاته ومراسلاته مع قادة جيوشه. وظهرت فيما بعد العديد من الآلات التي تقوم بعمليات التشفير كآلة (Enigma)، وشكّل الحاسب الآلي في بدايات ظهوره وسيلةً جديدة للاتصالات الآمنة، وفك تشفير رسائل العدو (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

واحتكرت الحكومات في فترة الستينيات حق التشفير وفك التشفير، وفي أواخر الستينيات، أسَّست شركة (IBM) مجموعةً تختص بأبحاث التشفير، ونجحت هذه المجموعة في تطوير نظام تشفير أطلقت عليه إسم Lucifer، ورغم اعتقاد الحكومة الأمريكية بعدم حاجة المؤسسات والمؤسسات الخاصة إلى نظم التشفير إلا إنه قد حقق انتشاراً واسعاً في الأسواق، ومنذ ذلك الحين أخذت العديدُ من المؤسسات بتطويرَ نظم تشفير جديدة مما أبرز الحاجة إلى وجود معيار لعمليات التشفير، ومن أبرز المؤسسات التي أسهمت في هذا المجال المعهد الوطني للمعايير والتقنية (NIST) National Institute Of Standards And Technology المعروف سابقاً باسم المكتب الوطني الأمريكي للمعايير U.S. National Bureau Of Standards، إذ طوَّر هذا المعهد عام ١٩٧٣م معياراً أطلق عليه معيار تشفير البيانات (DES)

Data Encryption Standards ويستنِد هذا المعيار إلى Algorithm Lucifer التي تستخدِم مفتاح تشفير بطول (٥٦) بت، وتشترط أن يكون لكل من المرسِل والمستقبل المفتاحَ السري ذاته. وقد استخدمت الحكومة هذا المعيار الرسمي عام ١٩٧٦م واعتمدته البنوك لتشغيل آلات الصراف الآلي ATM (Itep, D, ٢٠٠٢).

وبعد عام واحد من تطبيق معيار تشفير البيانات DES طوَّر ثلاثة أساتذة جامعيون نظامَ تشفير آخر أطلقوا عليه إسم RSA، ويستخدم هذا النظام زوجاً من المفاتيح، مفتاح عام Public Key، ومفتاح خاص Private Key عوضاً عن استخدام مفتاح واحد فقط. ورغم أن هذا النظام كان ملائماً جداً لأجهزة الحاسب الآلي المعقَّدة، إلا إنه قد تم اختراقه فيما بعد. وفي عام ١٩٨٦م قام Phil Zimmerman بتطوير برنامج تشفير يعتمد نظام RSA ولكنه يتميز باستخدام مفتاح بطول (١٢٨) بت ويُدعى برنامج الخصوصية المتفوِّقة (Pretty Good Privacy- (PGP، ويمكن استخدام ثلاثة طرق للتشفير كالتالي (Itep, D, ٢٠٠٢):

١. الشهادات الرقمية

تصدُر الشهادات الرقمية Digital Certificates عن الجِهات المانحة Certificate Authorities- CA الموثوق بها التي توقِّع عليها وتُستَخدَم هذه الشهادات للتحقُّق من موثوقية المفاتيح العامة التي أُصدِرَت. وفي البداية يقوم شخص أو شركة بتوليد زوج من المفاتيح العامة/الخاصة ثم يُرسَل المفتاح العام إلى جهة مانحة للشهادة CA وتُضيف الجهة المانحة CA بعضَ المعلومات المتعلِّقة بالشهادة مثل: الاسم ورقم التعريف No. ID وعنوان البريد الإلكتروني Email Address وتاريخ الانتهاء Date Expiration والرقم التسلسُلي Serial No وتُوقِّع عليها بالمفتاح العام لطالب الشهادة وبالمفتاح الخاص للجهة المانحة للشهادة Ca ويصادِق توقيع الجهة المانحة للشهادة Ca على المعلومات المُضافة إلى الشهادة وعلى المفتاح العام الموجود ضمن الشهادة ويمكن أن ترسِل الجهةُ المانحةُ الشهادةَ إلى طالبها أو تنشرَها للعموم أو تحتفظ بها. ولِفكّ شفرة الوثيقة المصدَّقة رقمياً

Digitally Certified Document تستخدِم البرمجياتُ في الطرف المستقبل المفتاحَ العام للجهة المانحة للشهادة Ca، وبعد تحقُّق كل طرف من الطرف الآخر يتَّفِق الخادم والمستفيد على معيار التشفير الذي سيُستَخدَم في جلسة تبادُل البيانات وفقاً لبروتوكول الطبقات الأمنية Data Exchange SSL Session.

٢. البصمة الإلكترونية

رغم أن التشفير يمنع من الاطلاع على محتويات الرسالة، إلا إنه لا يمنع المجرمين من العبث بها؛ أي إن التشفير لا يضمن سلامة الرسالة Integrity ومن هنا ظهرت الحاجة إلى البصمة الإلكترونية، وهي بصمة رقمية يتم اشتقاقها وفقاً لخوارزميات معيَّنة تُدعى دوالّ أو اقترانات التمويه (Hash Functions) إذ تطبِّق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة (سلسلة صغيرة) تمثِّل ملفاً كاملاً أو رسالة (سلسلة كبيرة). وتُدعى البيانات الناتجة البصمة الإلكترونية للرسالة Message Digest. وتتكوَّن البصمة الإلكترونية للرسالة من بيانات لها طول ثابت (يتراوح عادة بين ١٢٨ و١٦٠ بت) تؤخَذ من الرسالة المحوَّلة ذات الطول المتغير. وتستطيع هذه البصمة تمييز الرسالة الأصلية والتعرُّف عليها بدقة، حتى أي تغير بالرسالة- ولو كان في بت واحد- سيفضي إلى بصمة مختلفة.

٣. التوقيع الرقمي

يستَخدَم التوقيع الرقمي Digital Signature للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل ويمكن للمرسِل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونياً. أما في طرف المستقبل فيتم التحقّق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب. وباستخدام التوقيع الرقمي يتم تأمين سلامة الرسالة والتحقّق من صحتها. ومن فوائد هذا التوقيع أنه يمنع المرسِل من التنكّر للمعلومات التي أرسلها .

٣-٢-٢-٤ استخدام كلمات المرور

يتطلب أمان نظم المعلومات استخدام كلمات مرور معقدة لتسجيل الدخول إلى شبكة أو حاسب الآلي، ويمكن أن تكون كلمة المرور الارتباط الأضعف في النظام، وتكون كلمات المرور القوية هامة على اعتبار أن أدوات اكتشاف كلمات المرور مستمرة في التحسن وعلى اعتبار أن أجهزة الحاسب الآلي المستخدمة لاكتشافها أصبحت أكثر فعالية منذ قبل، وأصبح بالإمكان الآن كسر كلمات مرور الشبكة في ساعات بعد أن كان ذلك يستغرق أسابيع ولجعل كلمة المرور قوية يجب أن تكون ذات الموصفات التالية :(NOR٢٠٠٠, ٢٠٠٢)

١. أن يكون طولها (٨) أحرف على الأقل فإن أكثر كلمات المرور أماناً تكون بطول (٨) أحرف إلى (١٥) حرفاً، ويمكن أن يصل طول كلمات المرور Windows إلى (١٢٧) حرفاً، ولكن إذا كانت كلمة المرور أطول من (١٥)، وكان هناك اختلاف في نظم التشغيل فربما لن يكون بالإمكان تسجيل الدخول إلى شبكة الاتصال من أجهزة الحاسب الآلي هذه.
٢. أن تحتوي على أحرف من مجموعة الأحرف (A, B, C... a, b, c) ومجموعة الأرقام (٠, ١, ٢, ٣, ٤, ٥, ٦, ٧, ٨, ٩) ومجموعة رموز (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , .)
٣. أن يكون فيها على الأقل حرف رمز واحد في الموضع الثاني حتى السادس.
٤. أن تكون مختلفة كثيراً عن كلمات المرور السابقة.
٥. أن لا تتضمن إسم المستخدم، أو إسم أحد أفراد عائلته، أو أي معلومات عنه كرقم هاتفه، ورقمه الوظيفي.
٦. أن لا تكون كلمة شائعة أو اسماً شائعاً.
٧. يجب أن لا تكون هي نفس إسم الدخول.
٨. استخدم كلمات صعبة وغير موجودة في القواميس.
٩. عدم كتابة كلمة المرور (على ورقة مثلاً)، بل حفظه بالذاكرة الشخصية.

١٠. عدم التشارك في كلمة المرور الخاصة بالمستخدم مع أي شخص آخر.

١١. عدم استخدام كلمة المرور بتسجيل للدخول إلى شبكة الاتصال لأي غرض آخر.

١٢. استخدم كلمات مرور مختلفة لتسجيل الدخول إلى شبكة الاتصال وإلى حساب المسؤول الحاسب الآلي الخاص بك.

١٣. تغير كلمة المرور كل (٣٠) إلى (٦٠) يوماً أو كما هو مطلوب في البيئة الخاصة بالمؤسسة.

١٤. تغير كلمة المرور مباشرةً في حالة التوقع بأنه تم اكتشافها.

١٥. عدم حفظ كلمات المرور في جهاز الحاسب الآلي مثل مربعات الحوار التي تطلب حفظ كلمة المرور دائماً.

٣-٢-٣ السياسة الأمنية

تعد السياسة الأمنية Security Policy مجموعة من القوانين والقواعد والممارسات التي تضبط كيفية أداء المؤسسة لأعمالها, وكيف تقدم خدماتها لتحقيق أهدافها في ظل الأمن، وأحد الأغراض الرئيسية للسياسة الأمنية الوقوف على حجم التّهديدات التي تهدد المؤسسة والتي يجب أن تتجنبها وكيفية معالجة التهديدات بعد وقوعها.

١-٣-٢-٣ متطلبات تصميم السياسة الأمنية

تصميم السياسة الأمنية في المؤسسات يحتاج إلى إيجاد لوائح جوهرية لأمن المعلومات تكون متطابقة مع المواصفات الأمنية القياسية لمساعدة تلك المؤسسات في حماية معلوماتها (الشدي، ١٤٢١هـ: ١٥٠). وتصميم السياسات لتناسب الاحتياجات المختلفة للمؤسسة استناداً إلى القياسات العالمية للآيزوBS٧٧٩٩/ISO١٧٧٩٩، التي توفر إرشادات عامة لإدارة أمن المعلومات. وبعد تنقيحها وتضمينها للإجراءات الموجودة في المؤسسة، فإنها تصبح بمثابة التعليمات المستديمة لتعامل مع المعلومات الحساسة بشكل آمن (العِلم لأمن المعلومات، ١٤٢٣هـ). ويجب مراعاة تحديد مستوى الأخطار الواجب التغلب عليها وتحليلها ومن ثم تحديد الإجراءات التطبيقية

والتنظيمية الضرورية الواجب تغييرها لصياغة السياسة الأمنية (Comguard, ٢٠٠٢). يجب أن تتسم السياسة بالوضوح والسهولة بحيث يمكن من فهمها لجميع العاملين وخصوصاً غير المتخصصين (Castro, ٢٠٠٠). وعند تطبيقها يجب العمل على تقييمها بعد التنفيذ لمعرفة مدى القصور فيها لتلافيه (Comguard, ٢٠٠٢).

٢-٣-٢-٣ خصائص السياسة الأمنية

توفر السياسة الأمنية للمؤسسات هيكلاً لاتخاذ قرارات محددة، في كيفية شكل الخدمات المقدمة، وإجراءات المستفيدين، ومدراء النظام، لتحقيق أمن المعلومات في تلك المؤسسة (CERT, A, ٢٠٠٢). وتخاطب السياسة الأمنية كافة المستويات كلٌ بما يخصه (الإدارة العليا High-Level، والمشرفين Supervisor والمتخصصين Technician والمستخدمين Users) (Castro, ٢٠٠٠). كما تكون السياسة الأمنية مرجعاً قوياً في حالة حدوث الكوارث التي تهدد النظام المعلوماتي والتي بإتباعها يقل حجم الأضرار الناتجة عن حدوث تلك المهددات بعد وقوعها وتحديد الإجراءات لتلافي تكرارها (Barman, ٢٠٠١).

وتحدد السياسة الأمنية ما هو المسموح به وغير المسموح به من الأعمال والتي بناءاً عليها تتم معاقبة المخالف (Castro, ٢٠٠٠). وتعد السياسة الأمنية المرشد لمدراء النظام المعلوماتي في كيفية إدارة ذلك النظام، وتحدد الاستخدام المقبول للمستخدمين (CERT, A, ٢٠٠٢)، كما تحدد طبيعة الأعمال بالمؤسسة من واجبات وإجراءات (Castro, ٢٠٠٠). وتمد القانون بالقوة بتوضيحها وتسهيلها الكشف عن الجرائم وتحديد شخصية مرتكبيها لتقديمهم للعدالة، وبما توفره من وسائل تتبع للمخترقين، أو المخربين الذين يقومون بتعطيل وعمل تغييرات على النظام المعلوماتي (CERT, A, ٢٠٠٢).

كما تحدد السياسة الأمنية مدى انفتاح المعلومات Accessible Information لوسائل النشر وللأشخاص الذين لا ينتمون للمؤسسة أومن أقسام أخرى داخل المؤسسة (Barman, ٢٠٠١)، وتحدد

طرق تنظيم البيانات والمعلومات، كتحديد نوع السجلات المستخدمة، ونوعية المعلومات التي تحتويها (Castro, ٢٠٠٠).

٣-٢-٣-٣ مكونات السياسة الأمنية

يصعب تحديد مكونات السياسة الأمنية Security Policy Contents في ظل التغيرات السريعة بشكل التقنية، ورغم هذا فحاجة المؤسسات لأمن نظم المعلومات تعد أمراً ضرورياً، مما يترتب علية تحديد مكونات السياسة الأمنية وتضمينها العناصر التالية.

١. تحديد الغرض

تحديد الغرض المراد حمايته Determine purpose What Is to Be Protected كالأجهزة والبرامج والإجراءات، وهذا يساعد في صياغة الواجبات (Barman, ٢٠٠١). وتعتمد السياسة الأمنية على نوع التقنية المستخدمة، فالمؤسسات التي لا تستخدم الحاسب الآلي فإن سياستها الأمنية في مجال أمن المعلومات تتركز حول عدم خروج الأوراق من المؤسسة مثلاً، والمؤسسة التي لا تستخدم الإنترنت لا تسمح بخروج وسائط الحفظ، وإغلاق غرف الحاسب الآلي، وأما المؤسسات التي تستخدم الإنترنت فإن الفائدة من منع الخروج بوسائط الحفظ غير عملي إذا لجاء المستخدمون إلى استعمال وسائل نقل البيانات إلكترونياً كوسيلة البريد الإلكتروني. ولهذا فإن السياسة الأمنية تبنى على معرفة مكونات النظام المعلوماتي، وتستخدم كل مؤسسة احتياجاتها من التقنية مع مراعاة أمنها. ولا يغيب عن صانعي السياسات الأمنية انه لا توجد حماية كاملة، فارتباط الحاسب الآلي بالطاقة الكهربائية أكثر خطورة من كونه مفصول، وارتباط الحاسب الآلي بشبكة الداخلية أكثر خطورة من كونه غير مرتبط، وارتباطه بالإنترنت أكثر خطورة مما سبق، وعلى ضوء ما سبق من تحديد ماذا يُحمى، فإنه لا بد من تحديد عن من تحمى.

٢. تحديد المجال

يشمل تحديد المجال تحديد من الذين يطبقونها، وعلى من يطبقونها، وما هي أنواع الأجهزة المستخدمة والتي تشملها (حاسبات صغيرة، كبيرة متوسطة) وما هي وسائط الاتصالات (مودم، مكررات، جسور) وما هي نظم التشغيل في الأجهزة والشبكات، ومحطات العمل، ومنطقة امتدادها، وما تشمله من إجراءات، وعلاقات مع كافة المتعاملين في مجال النظام المعلوماتي، والعاملين والمواقع الوظيفية لهم وامتداد أعمالهم، وتحديد امتداد بيئة النظام (Castro, ٢٠٠٠).

٣. تحديد عناصر السياسة الأمنية

بعد تحديد عناصر السياسة الأمنية التي تحتاجها المؤسسة يجب أن تشمل تلك العناصر توجيهات وأوامر إلى الأفراد العاملين بالمؤسسة في كل عنصر من عناصر السياسة الأمنية ويكون مفادها (إفعل أو لا تفعل). وبشكل عام سوف يتم التطرق إلى بعض العناصر المهمة التي تحتاجها غالبية المؤسسات على النحو التالي:

أ. الموقع المكاني لخدمات تقنية المعلوماتية: يتم تحديد الإجراءات للدخول على موقع المكاني لخدمات تقنية المعلوماتية، وتحديد المعدات المادية والتقنية والتي يجب استخدام لتأمين الموقع، بالإضافة إلى تحديد واجبات الحراسات (Barman, ٢٠٠١). يجب تحديد خطط مواجهة الكوارث، والإجراءات التي يطلبها النظام المعلوماتي حين وقوع الكوارث وبالتفصيل كشرح أهداف الخطة، وطرق مواجهة الكوارث، ونقل البيانات، ووسيلة الإنذارات، كما يجب أن تتضمن مواصفات المباني الخاصة بالأجهزة، وسلامتها من حدوث المخاطر، وسياسات بناء المرافق الجديدة أو مركز الاتّصالات وأيضاً طريقة الدخول للمبنى، والعمل على تفريغ الكهرباء السّاكنة، ومراعاة التكييف، كما يجب أن تتضمّن السّياسات السيطرة على مداخل مركز الحاسب الآلي، وتعد هذه السيطرة فقط للحفاظ على الأمن المادي من التدخل البشري المباشر (Castro, ٢٠٠٠).

ب. كلمات المرور: يجب أن تحتوي السياسة Password على تحديد طريقة توليف كلمات المرور، وتحديدها بنمط يلائم الوظيفة التي ستمنع من يمنح كلمة المرور من استخدام كلمات مرور يمكن أن تتضمن أسماء خاصة أو متداولة، وخصوصاً في بعض المؤسسات ذات المعلومات الحساسة كالمعلومات العسكرية، وقد يعمد والتي يكون توليد كلمة المرور للمستخدم عادة تؤلف باستخدام عدد من الأسماء الصّالحة للنّشر أو توليف كلمات مرور أكثر تشويقاً إلى المستخدمين، ولسوء الحظ أن هذه الكلمات تكون أكثر سهولة لتذكر (Barman, ٢٠٠١).

ج. الوثائق ووسائط الحفظ: توضح أسلوب حفظ النسخ الاحتياطي Backups، ووسائط الحفظ Archival Storage، وإتلاف البيانات Disposal Of Data، وتهدف هذه الحماية للمحافظة على المعلومات من التلف Crashes ولحفظ المعلومات للأوقات الحرجة Preserve Critical Data، وتعالج الحفظ الداخلي للبيانات، وطريقة إعداد النسخ والفترة الزمنية للحفظ (يومي، أسبوعي، شهري)، وإجراءات المراجعة Review، والتدقيق Verify، وتحدد الطرق والأدوات المستعملة في إتلاف البيانات Discard (Barman, ٢٠٠١).

د. الجانب البشري: تتضمن السياسة الأمنية التحري الدقيق عن كل شخص يتقدم لوظيفة ترتبط بمركز المعلومات في المؤسسة وخاصة المبرمجين، ومحللي نظم المعلومات (السحيباني، ١٩٩٧م: ٤٤). وتورد في مضمونها التعليمات لكافة المستويات الإدارية، وجميع التخصصات، بتحديد الواجبات المتعلقة بالوظيفة، والإجراءات التي يمكن تطويرها باستمرار لتكفل سرعة الأداء وتبسيط الإجراء لإنجاز المهام المنوطة بالمؤسسة. وتعد السياسة الأمنية تشريعات داخلية تحدد وصفاً للقيام بجميع الأعمال، وتقرير العقوبات وتوقيعها على المخلين بأمن المعلومات.

هـ. البرامج الجاهزة: لابد من قيام المؤسسة باختبار البرامج الجاهزة ومدى ملاءمتها للقيام بالأعمال المنوطة بها مع مراعاة الجانب الأمني للأداء، والعمل على تحديث تلك البرامج من بيئة الإنتاج (Barman, ٢٠٠١).

و. التشارك في الخدمات: تحديد الموارد المعرضة للتشارك، وإعطاء الصلاحيات للعاملين حسب الهيكل التنظيمي للمهام والاستفادة من الموارد، وتضمين السياسة استخدام تطبيقات تقوم بمراقبة منافذ التشارك في الموارد، ولسد ثغرة التشارك في الملفات والطباعة مع إبقائهما نشطتين في حالة الشبكات. يجب استخدم جداراً نارياً مزوداً بخاصية سد المنافذ مثل Black Ice Defender أو حذف كلمات المرور من PWL بواسطة برنامج WAPS (المجلة الإلكترونية، ١٤٢٣هـ).

ز. الاحترازات الشخصية: تضمين السياسة الأمنية عدم إدخال أو إخراج أي جهاز حاسب الآلي أو جهاز أخر أو وسائط حفظ بدون إذن المؤسسة، كما يجب التنبيه على الموظفين بعدم إحضار أي أجهزة شخصية لهم داخل المؤسسة، أو وسائط حفظ، كما يجب تضمينها إلزام الموظفين بحفظ النسخ الاحتياطي بطريقة آمنة، والمحافظة على وسائط الحفظ، وتأمين الأجهزة بما يضمن عدم اختراقها من أي مصدر.

ح. العلاقة بالمنافسين والشركاء: يجب أن تتناول السياسات الأمنية الاتفاقيات والشروط بين المؤسسات وبين المنتجين والموردين للتقنية، والجهات التي تقوم بتجهيز وتركيب العتاد داخل المؤسسات. وعليهم فهم واحترام السياسات الأمنية للمؤسسات والعمل على إنتاج وتوريد، وتصدير، وتركيب ما يدعمها، وعدم الإخلال ببنود العقود. والتي تتطلبها السياسة الأمنية (Barman, ٢٠٠١). ويجب أن يكون هناك اتفاقيات تنظم الأعمال المشتركة بين الشركاء، وما تفعله الشركة باتجاه المنافسين كأن تمنع موظفيها (حتى ولو خارج العمل) بالذهاب أو العمل أو الدعاية لمنتجات وخدمات المنافسين، أو استعمالها.

ط. تطوير البرامج: سياسات تطوير البرامج Software Development Policies تعالج الأخطاء المقصودة، وغير المقصودة في تطوير البرامج يمكن أن تؤدي إلى نتائج مأساوية. وبعض المؤسسات ليس لديها خبرة كافية لتطوير البرامج فتلجأ إلى طرف ثالث، فقد يكون مصدراً للأخطار الأمنية التي يمكن أن تتعرّض لها المؤسسة. ويجب عدم الوثوق بالبرامج التي منشأها

التطوير. ويلزم مراعاة نواحٍ عدة في عمليات تطوير البرامج أثناء تّصميم وتطوير البرامج وذلك بوضع القواعد الأساسية لتطوير برامج آمنة تتوافق مع آليّات نظم التّشغيل وقاعدة البيانات أو البرامج المساعدة، ومعرفة ما المفترض الذي يمكن أن يتم تركيبه على النظام والشبكة وعدم تركيب البرامج المخالفة التي تخل بأمنه (Barman, ٢٠٠١).

ي. استخدام الإنترنت: من الضروري فهم الأسس البنائي لشبكة وكيفية عمل الحاجز الناري والبرتوكولات العاملة بالشبكة المحلية المربوطة بشبكة الإنترنت التي يمكن أن تلعب دوراً في تصنيف الخدمات المقدمة سواء كانت خدمات داخليّة أو خارجية، وتضع تصوراً في أمن الإنترنت، يعتقد المستخدمون أنهم لا يحتاجون إلى التّدريب للوصول إلى الإنترنت، ولكنّ ينبغي أن يتدربوا عليها، ويشرح لهم مسئوليّاتهم الملخّصة بالسّياسة الأمنية، ولا يتم استخدام الإنترنت إلا وفق احتياجات المؤسسة ومنع منسوبيها من الاستخدامات غير ضرورية كزيارة المواقع المتنوّعة على الإنترنت (Barman, ٢٠٠١).

تعتمد معظم المؤسسات على معلومات خاصة أو حساسة فيجب أن تكون السياسة قائمًا لشرح معالجة هذه المعلومات وفق ضوابط وحماية تكفل عدم الإخلال بأمن المعلومات، وينبغي أن تحظر هذه السّياسات تحميل البرامج من مواقع بالإنترنت، وتشرح للمديرين إجراءات تحميل تلك البرامج، وتلزم بتزويد المواقع بوسائل الحماية وخصوصاً عندما يكون الموقع مرتبط بشبكة الداخلية للمؤسسة. ولي استمرارية عمل الموقع لابد من تضمين السياسات الأمنية صيانة برامج ودعم المواقع. كما يجب أن تحكم السياسات في محتوًى المعلومات على موقع الإنترنت، وتحديد ما هي المعلومات المناسبة وضع سياسات لما تعمله المؤسسة بالمعلومات التي جمعتها من خدمات الموقع حتى لا تستغل لإغراض خاصة (Barman, ٢٠٠١).

ك. استخدام البريد الإلكتروني: يجب وضع سياسة أمنية لاستخدام البريد الإلكتروني Email Policies Security الذي يساند أهداف المؤسسة، ومطالب التّجارة الإلكترونية. وتتطلب

سياسة البريد الإلكتروني وصف الأعمال التي تتبع في إدارة نظام البريد الإلكتروني، وتحديد من الذي له الأحقية بمسح الرسائل، وتحديد حجم الرسائل لمنع ازدحام الشبكة وتخفيف المشاكل الأخرى. وتعيين المفوّضين باستخدام البريد الإلكتروني، ورصد الوسائل المساعدة في إرسال الرسائل، وتوضيح طريق حفظ الرسائل، واستخدام الاتّصال الواثق بتشفير البيانات قبل الإرسال واعتماد التوقيع الرقمي (Barman, ٢٠٠١)

ل. الفيروسات والدّيدان وأحصنة طّروادة: تكون هناك حاجة للحماية من الفيروسات والدّيدان وأحصنة طّروادة and Trojan Horses ,Viruses, Worms وهذا يتطلب أن تتضمن السياسة كل ما يؤدي لعدم الإصابة بها كمنع نسخ البرامج من المصادر غير موثوقة، كما يجب أن يكون هناك توضيح من قبل المنتجين بحالة حماية برامجهم بفيروسات (Castro, ٢٠٠٠).

٣-٣ جرائم نظم المعلومات

تُعرّف الجريمة بأنها حدث على شكل سلوك ودوافع، يحركه مثير وينشطه يؤدي إلى استجابة على شكل سلوك غير مادي، وسلوك يمكن أن يكون على شكل (فعل، تفكير، عواطف) وهي مرتبطة بالسلوك الناتج عن الفرد، ويحددها المفهوم القانوني الذي يرتبط بالحدود القانونية، ويشمل الحدود المعيارية القيمة الموجودة في المجتمع، كما يحددها المفهوم الاجتماعي الذي يخالف المفهوم القانوني من حيث نقطة جوهرية ليس من كون الجريمة موجودة أو غير موجودة وإنما يخالفه أن المفهوم الاجتماعي لا يشترط وجود نص قانوني لتجريم الأفعال فعندهم الذي يجرم الفعل هو المجتمع، كما أن درجة التسامح في المجتمعات تجاه بعض السلوكيات مختلفة، فهناك مجتمعات درجتها متوسطة، والأخرى شديدة، فالانحراف هنا مرتبط "بالحدود التسامحية" (طالب، ١٤٢٠هـ: ٧).

ويجمع فقها القانون الجنائي على اعتبار أن الجريمة سلوك يحظره القانون ويرتب عقوبة لمرتكبه. ومن التعريف القانوني للجريمة على أنها عمل إي عمل يجرِّمه القانون أو امتناع عن عمل يقضى به القانون (عوده، ١٤٠١هـ)، نجد عدم اعتبار الأعمال غير المشروعة جريمة في نظر القانون إلا إذا كان العمل غير المشروع مجرماً ومعاقباً عليه، وينطلق القانون في تجريمه للأعمال غير مشروعة بأن العمل غير المشروع يُحِدّث ضرراً سواء كان هذا الضرر ضد فرد أو جماعة أو مؤسسة، وبتجريمه لتلك الأعمال غير المشروعة يضمن القانون عند تطبيقه بشكل المطلوب المحافظة على عدم تداخل الحريات وتصادمها مع بعضها البعض لما يمنع مزيد من الجرائم ويكفل استقرار الأمن للمجتمع.

أن تعريف الجريمة وتحديد أركانها ومعرفة عناصرها وأنماطها وأساليبها، وأدوات ارتكابها له أهمية خاصة عند رجال القانون والعاملين في جمع الأدلة الجنائية. الذين يسعون دائماً لإثبات أركان الجريمة وعناصرها، وإيجاد العلاقة بين أركان الجريمة والشخص المتهم بتنفيذ تلك الأركان (البشري، ١٤٢١هـ: ١٨). ولأهمية بيان أنماط جرائم نظم المعلومات، وأساليبها، وأدوات ارتكابها، ودوافعها، لكشف مرتكبيها يستعرض الباحث تلك العناصر بالتفصيل.

٣-٣-١ أنماط جرائم نظم المعلومات

"من الصعب حصر أنماط جرائم نظم المعلومات بسبب التطور في صناعة التقنية إلى أن غالبيتها تم تحديد مصطلح له وقليل منها تم وضع عقوبة له" (البشري، ١٤٢١هـ: ١٨). وبالنظر إلى بعض المصطلحات التي تدخل تحت مسمى جرائم التقنية وهي؛ مصطلح Cyber Crime الجرائم الإلكترونية، ومصطلح Computer Abuse الاستعمال الخاطئ للحاسب الآلي، ومصطلح Misuse Compute إساءة استخدام الحاسب الآلي، ومصطلح Computer Related Crime الجرائم المتعلقة بالحاسب الآلي، ومصطلح Crime Computer جرائم الحاسب الآلي، ومصطلحFraud Computer احتيال الحاسب الآلي، ومصطلح Computer Forgery تزوير الحاسب الآلي، ومصطلح Computer

Sabotage تخريب الحاسب الآلي، ومصطلح Computer Espionage تجسس الحاسب الآلي، ومصطلح Information Systems Crime جريمة نظم المعلومات، ومصطلح Internet Crime الجرائم التي ترتكب عن طريق شبكة الإنترنت (المسند، والمهيني، ١٤٢١هـ: ٣٣٦)، نجد إن تلك المصطلحات السابقة استخدمت للدلالة على نمط تلك الجرائم ولم تضع حداً فاصلاً بين ما يشمله كل مصطلح من جرائم عن المصطلح الأخر، ولا تتضمن تفصيل بين المقصد العمدي والاستخدام الخاطئ العفوي والاستخدام الخاطئ نتيجة الإهمال أو الاستخدام الخاطئ المتعمد أو الاستخدام الخاطئ الذي يرقى إلى سوء الاستخدام (عبد المطلب، ٢٠٠١م:). وفي عام ١٩٨٩م وضعت اللجنة الأوربية لمشاكل الجريمة بالمجلس الأوربي التابع للأمم المتحدة إرشادات عامة بشأن الجريمة المعلوماتية وتصنيفها، وقد أشارت الأمم المتحدة في مدونتها التي أصدرتها بشأن الجريمة المعلوماتية إلى خلاف الخبراء حول تحديد هذه المصطلحات، وتركت للدول المعنية مسألة تكييف الوضع القانوني بما يتفق مع كل نظام دولة وتقاليدها (IFS, ٢٠٠١).

ويمكن تقسيم أنماط الجرائم المتعلقة بالنظم المعلومات حسب أسلوب استخدامها، فالنوع الأول استخدام تلك الأداة (حاسب، شبكة، ...الخ) وسيلة يرتكب بها الجريمة، والنوع الثاني عندما تكون هدفاً مثل (الحصول على معلومات، وتدمير معلومات...الخ) (البشري، ١٤٢١هـ: ١٣٧). كما يتم تقسيمها حسب هدف الجاني المباشر فقد تكون موجهه إلى المعلومات، أو الأشخاص، أو الأجهزة (الهاجري، ١٤٢٣هـ)، وهذا يتفق مع تقسيم القانون الفرنسي لأنماط الجرائم المعلوماتية (عبد الرحمن، ١٩٩٢م: ١٧٨)، كما سلكه كثير من الباحثين. وسوف يتم تناول الأنماط المطروحة بهذه الدراسة.

٣-٣-١-١ الاحتيال المعلوماتي Information Fraud

"انتشر الاحتيال المعلوماتي انتشاراً كبيراً، فتأثرت سلوكيات فئة كبيرة من الناس، في مقدمتهم الذين يتعاملون مع نظم المعلومات، لسهولة قيامهم به، وبعدم توفر نظام أمني خاص يحول

دون اقترافهم لتلك الجرائم" (شتا، ٢٠٠١م: ٧٠). يدخل تحت الاحتيال المعلوماتي التلاعب بإدخال البياناتData Didding الذي يعتمد على إدخال بيانات لا وجود لها أصلاً أو بيانات محرفة أو تنطوي على الأمرين، وقد تستمر فترة طويلة دون أن تكتشف (شتا، ٢٠٠١م: ٨٠). وتغيير البيانات بعد إدخالها الذي يتم تعديلها أو تغيرها وإبقاءها بشكل مستمر للاستفادة منها أو تركها لفترة محدودة لإرسالها أو طباعتها وبعد ذلك يتم أعادتها لوضعها السابق، كما يدخل تحته النسخ غير المرخص للبيانات للاستفادة منها، كما يدخل تحت الاحتيال المعلوماتي استخدام برامج مخصصة لإغراض محددة كبرنامج Super Zap المطور لاستخدامه في حالة الطوارئ لتجاوز قيود التحكم العادية وتنفيذ عمليات غير مشروعة (المسند، والمهيني، ١٤٢١هـ: ١٨٣).

كما يدخل تحته برمجة النظم والتطبيقات بطريقة تحقق للمبرمج مصالح شخصية غير مشروعة كاستغلال المؤسسات المالية التي تدفع الفائدة، ويتم بطريقة تقريب الأرقام، وكأسلوب السجق (سلامي) أي سرقة المال بمقدار بسيط على فترات طويلة، ويدخل تحت الاحتيال المعلوماتي تغير الإعدادات لتسمح بتجاوز قيود التحكم المعتاد في النظام، وغالباً توضع الإعدادات على وضع معين أثناء تطوير النظام، ثم تحذف قبل وضع النظام بشكل التشغيل النهائي (المسند، والمهيني، ١٤٢١هـ). كما يدخل تحت هذا النوع، "القنبلة الموقوتة وهي تعليمات غير مرخصة موضوعة في برنامج بهدف إجراء عمليات غير مشروعة في وقت محدد مسبقاً حين تحقق شروط معينة" (المسند، والمهيني، ١٤٢١هـ: ١٨٢).

٢-١-٣-٣ تدمير الملفات وقواعد البيانات

إن الهدف المباشر للتدمير هو المعلومات المخزنة على الأجهزة المقتحمة حيث يتم إفسادها، أو تغييرها أو حذفها أو سرقتها ونقلها إلى أجهزة أخرى (الهاجري، ١٤٢٢هـ). تتمكن أدوات التدمير من الدخول إلى النظم عبر البريد الإلكتروني، ومن خلال خاصية مشاركة الملفات File

Sharing، ومحركات الأقراص، وبرامج المراسلة الفورية Instant Messaging Program، ومواقع الإنترنت (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

٣-٣-١-٣ التجسس الإلكتروني

التجسس Spy: اصطلاحاً، هو: البحث والتنقيب عما يتعلق بالعدو، من معلومات سرية باستخدام الوسائل السرية والفنية، ونقل ذات المعلومات بذات الوسائل، أو بواسطة العملاء والجواسيس، والاستفادة منها في أعداد الخطط. أما الجاسوسية قانوناً، فهي؛ العمل سراً وبادعاء وهمي لمحاولة الاستيلاء على معلومات سرية بقصد إبلاغها إلى جهة معادية، تطور التجسس في عصرنا هذا، وأصبح من الممارسات اليومية التي تعتمد عليها الدول في حماية أمنها، وتطوير صناعاتها، بل وفي التعامل مع أصدقائها (Geocities, ٢٠٠٢).

تتجسس الدول اليوم على منافسيها، بجمع المعلومات عن مصادر القوة ومواطن الضعف لديها في السياسة والاقتصاد، وعن درجة الوعي والروح المعنوي في المجتمع، وحركة الجند، والقوة العسكرية، وعن تجمعات الدول الصديقة وتحالفاتها، والى أي مدى تتكامل المصالح أو تتناقض يحين التحالف بين دولتين صديقتين ضد طرف ثالث (Geocities, ٢٠٠٢). نتج عن ازدهار صناعة تقنية المعلومات وانتشارها في السنوات القليلة الماضية، تسهيل لمهام التجسس المعلوماتي بين الدول، التي تعتمد على عناصر يعملون داخل الجهة الأخرى للحصول على معلومات حساسة، بقيامهم من داخل المؤسسة بسرقة معلومات سرية وإرسالها إلى الجهة المستفيدة بوسائط الإنترنت، أو الحصول على المعلومات بالتجسس من بعد بأدوات خاصة. ويمكن للشخص قليل الخبرة الحصول على عدة أدوات تجسسية من مواقع كثيرة على شبكة الإنترنت، ويمكنه استخدامها لدخول على الأجهزة المرتبطة بالشبكة وإحداث أشكال مختلفة من التخريب، والسرقة، والتعطيل (الهاجري، ١٤٢٣هـ)، أو نقل المعلومات إلى المصدر عن طريق النظم لما توفره من سرية فائقة (الإيهم،

١٤٢٣هـ). كما أصبح التجسس أكثر خطراً، بتأثير التقدم التقني، الذي وفر أجهزة ومعدات غاية في الدقة، وصغر الحجم، ودرجة الكفاءة في التنصت، والاستشعار من بُعد (Geocities, ٢٠٠٢).

٤-١-٣-٣ تشويه المواقع Defacement

من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم، هي تلك التي تستضيف المواقع على الإنترنت، حيث يتم تغيير المعلومات الموجودة على الموقع. إن استهداف هذا النوع من الأجهزة يعود إلى كثرة وجود هذه الأجهزة على الشبكة وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة (الهاجري، ١٤٢٢هـ). وتشويه المواقع يتم بتغيير الصفحة الرئيسية وتتم عملية التشويه باختراق مزودات Web، ويقصد المخترق من ورائها انتصاره على نظام مزود Web والإجراءات الأمنية للشبكة وإبراز قدراته التقنية وإعلان تحديه للمشرفين على نظم مزودات Web ليثبت لغيره امتلاكه المقدرة التقنية على كسر نظام الحماية في هذه المزودات. وتتضمن أهداف من يقوم بعملية التشويه إيصال رسالة للعالم كاعتراضه على حالة سياسية أو اجتماعية أو صرخة يريد إيصالها إلى كل من يزور الموقع. ويؤدي هذا العمل على الإضرار بسمعة الجهة المالكة للموقع (khalal٢٢, ٢٠٠٢).

بلغ عدد عمليات تشويه المواقع، التي رصدت في أنحاء العالم منذ العام ١٩٩٥م وحتى ١٩٩٩م حوالي (٥٠٠٠) عملية توزعت على مختلف مواقع Web التي تملك أسماء نطاقات تجارية (Com ، Net، Org) في جميع دول العالم تقريباً، وتشير الدراسات إلى أن حوالي (٢٠٪) من عمليات التشويه تتم في أول يوم من العطلة الأسبوعية ويرجح السبب في ذلك إلى أن تغيير الصفحة الرئيسية في موقع معين يوم العطلة الأسبوعية (في معظم دول العالم) يضمن بقاء التغيير أطول مدة ممكنة إلى أن يعود مدير الشبكة وموظفو المؤسسات من إجازتهم ويعيدوا الصفحة الأصلية للموقع إلى ما كانت، وحدثت أوائل عمليات التشويه في العالم عام ١٩٩٥م ولم تتعدَ في ذلك الوقت أربع عمليات وتلتها (١٨) عملية العام ١٩٩٦م و(٢٨) عملية سنة ١٩٩٧م ثم تضاعفت عام ١٩٩٨م

ليصل العدد إلى (٢٣٣) عملية تشويه مواقع وفي سنة ١٩٩٩م تضاعف عددها حوالي (١٥) مرة ليصل (٣٦٩٩) عملية تشويه في مختلف أنحاء العالم، ومن ضمنها (١٦) عملية تمت على مواقع محلية في الدول العربية وكانت المواقع المحلية البرازيلية، أكثر دول العالم إصابة بعمليات التشويه، وبلغ عدد العمليات فيها (١٧٨) عملية تلتها الولايات المتحدة الأمريكية التي بلغ عدد العمليات فيها (١٢٦) عملية (khalal٢٢, ٢٠٠٢).

٣-٣-١-٥ تعطيل الأجهزة والمواقع (DDOS (Distributed Denial Of Service

تحدث هذه الهجمات باستخدام منافذ بروتوكولات TCP وUDP بالإضافة إلى ICMP في تسليط حزم شبكية إلى مزودات معينة عبر أوامر مثل Ping (CERT, A, ٢٠٠٢). ومن أشهر الهجمات تلك التي تستخدم نوع الهجوم المعروف باسم Win Nuke، والتي تسلط سيلاً من الحزم الشبكية عبر المنفذ (١٣٩) من نظام Net BIOS، الذي يسمح بتحاور التطبيقات الموجودة على الأجهزة المرتبطة بالشبكة، ويمكن دفع حزم شبكية إلى مزودات معينة لإيقافها عن العمل، سواء كانت مزودات Web أو مزودات بريد إلكتروني أو أي مزود يمكنه أن يستقبل الحزم الشبكية، وتعرف أنواع هذه الهجمات، بأسماء غريبة منها Smurf Syn، Floods، Land، Ping Bomb، Ping O'death، Fragile، Win nuke (Cisco. ٢٠٠٢).

وتشكل هذه الهجمات خطراً على شبكة الإنترنت كلها، وليس على بعض المواقع فقط، حيث أن كل موقع من المواقع التي أصيبت بهذا النوع من الهجمات، يحجز جزءاً كبيراً من حزمة البيانات على شبكة الإنترنت، مما قد يهدد بإيقاف شبكة الإنترنت بالكامل (khalal٢٢, ٢٠٠٢).

كما يتم تعطيل الأجهزة بإرسال بقة نظام التشغيل DOS يتم فيها استخدام لغة الترميز HTM، وزرع تعليمات وبرامج مستخدمة في نظام التشغيل DOS ليتم تعطيل نظام Windows، واكثر نظم التشغيل التي يمكن لها أن تتأثر بها هي نظام التشغيل ٩٥ , ٩٨ Windows لأنهما يعتمدان على DOS

١٦بت وفيه توجد بعض الأوامر التي تمكن نظام التشغيل من التعامل مع الأجهزة الملحقة وهي؛ LPT١ For Printer ، COM١, COM٢ For Communication And Fax Modem، وتسبب بعض المشاكل لأنها تجعل نظام Windows يتبادل المعلومات و الأوامر مع المكونات مثل الفاكس مودم و الطابعة بدلاً من القرص الصلب وبالتالي يتوقف الجهاز عن العمل (المجلة الإلكترونية، ١٤٢٣هـ).

٣-٣-١-٦ الإخلال بأمن المعلومات

تقع جرائم الإخلال بأمن المعلومات من خلال العاملين بالمؤسسة، إما بالقيام بها أو نتيجة تساهلهم، أي تكون متعمدة أو غير متعمدة، فعدم إتباع السياسات الأمنية الموضوعة لهم تعد إخلالاً بأمن المعلومات، كإفشاء كلمات المرور (المسند، والمهيني، ١٤٢١هـ: ٢٩٨)، أو عدم تطبيق متطلبة السياسة الأمنية بشأنها، أو سرقة وسائط الحفظ الخارجية نتيجة تساهل العاملين بالمؤسسة، أو نسخ البيانات والبرامج، أو تشغيل الأجهزة عن طريق القرص المرن للدخول غير مرخص على الأقراص الثابتة والحصول على البيانات، أو عدم متابعة إجراءات الصيانة حتى لا تتم زراعة برامج اختراق بواسطة موظفي الصيانة والتشغيل بالمؤسسة أو الحصول على البيانات السرية خلال أعمال صيانة الأجهزة، أو الاستخدام غير القانوني لأجهزة غير حين تركها غير مؤمنة.

٣-٣-١-٧ انتهاك الخصوصية

المؤسسات والمواقع كانت في السابق تقوم بجمع المعلومات اعتمادا على عنوان بروتوكول الإنترنت (IP) وذلك دون معرفة المستخدم شخصياً. أما الآن وبعد تطور التكنولوجيا التي تسمح لهم بأكثر من ذلك فإن العديد من المؤسسات والهيئات وبنوك المعلومات، قادرة على تحديد رقم هاتفه الذي يتصل منه وعنوانه وكذلك تسجيل كل ما يقوم بكتابته أو ما يستقبله في غرف الدردشة أو الرسائل الإلكترونية. ويمكنهم بيع هذه المعلومات لمؤسسات التسويق والدعاية أو الجهات الحكومية الأخرى في العالم نظم المعلومات (صلاح، ٢٠٠١م).

٣-٣-١-٨ انتحال شخصية

هي جريمة الألفية الجديدة كما أسماها بعض المختصين في أمن المعلومات وذلك نظراً لسرعة انتشار ارتكابها خاصة في الأوساط التجارية، تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى (الهاجري، ١٤٢٣هـ).

٣-٣-١-٩ التنصت على الشبكات

يتم باستخدام تقنيات معينة بسرقة المعلومات المارة أو يقوم بتعديلها، ويمكن أن يكون التنصت على أشكال عديدة، كتنصت مباشرة على أسلاك الاتصالات، أو استخدام أجهزة لالتقاط الإشعاعات من الحاسب الآلي، أو من موجات البث، أو زراعة أجهزة داخل الحاسب الآلي لتقوم بالتقاط البيانات الداخلة أو الخارجة والتقاط بث هذه الأجهزة عبر الأقمار الاصطناعية، أو التقاط البيانات المارة عبر الشبكات. فقد يقوم خبير في نظم الاتصالات وعن طريق استخدام أجهزة التنصت على أسلاك بين فرع وفرع لمعرفة حجم الأعمال، وغالباً تستخدم هذه الطرق بتجسس بين الدول (الشدي، ١٤٢١هـ: ٣٥).

٣-٣-١-١٠ اعتراض رسائل البريد الإلكتروني.

يتم إرسال بيانات البريد الإلكتروني غالباً ضمن رزم Packets عبر الشبكات، وهذا يعني أن رسالة البريد الإلكتروني لا يتم إرسالها كل رزمة بنفس المسلك الفعلي للرزم الأخرى، لذلك فأي شخص يريد اعتراض البريد الإلكتروني، يجب أن يمتلك خبرة تقنية عالية إضافة إلى خبرته في الوصول إلى الحاسبات الآلية وخطوط البيانات التي تتعامل مع الرسائل للإلكترونية، كما انه يجب علية أن يبذل مزيدا من الجهد لتعقب الرزم واعتراضها وإعادة تجميعها. وحالياً يتوفر تطبيق Packet-Sniffing على الإنترنت، حيث يستغله مخترقون غير بارعين، وهنا عامل الخطورة لأنه مع

وجود التطبيقات المناسبة وانتشارها بالإنترنت يسهل عمليات اعتراض البريد الإلكتروني بدون أي جهد أو مشقة (مجلة الأمن الإلكترونية، ٢٠٠٢م).

٣-٣-١-١١ الإغراق Flooding

يتم فيها استخدام برامج جاهزة خاصة لإغراق البريد الإلكتروني، والمتوفر بكثرة على الإنترنت، ما على المهاجم إلا وضع عنوان الرسالة subject، ونصها Text Body، وعدد مرات إرسالها times send، وعنوان المرسل إليه TO، وبعد ذلك ضغط أمر send أو Bomb. وتختلف عدد الرسائل اللازمة لإغراق بريد معين وذلك حسب نوع الموفر للبريد فالبريد المجاني ليس بقوة البريد المسجل تحت إسم شركة أو جهة حكومية، الذي يستطيع تحمل عدد هائل من الرسائل (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

٣-٣-٢ أساليب ارتكابها

يمكن حصر مجموعة من الأساليب كالاختراق المباشر للشبكات وأجهزة الحاسب الآلي المرتبطة، والاختراق المبطن، ورصد لوحة المفاتيح، وكسر كلمات المرور في أجهزة الحاسب الآلي، و IP Spoofing، وسوق يتم تناولها بالتفصيل.

٣-٣-٢-١ الاختراق المباشر للشبكات وأجهزة الحاسب الآلي المرتبطة

يعتمد على استغلال المنافذ المفتوحة بنظم التشغيل، أو برامج الحماية، والتي هي أساسها أخطاء برمجية بشرية، ويقع تحته مجموعة من الأساليب منها؛ البحث عن المنافذ المفتوحة عن طريق الشبكات، واستغلال المنافذ المفتوحة، وكسر كلمات المرور الخاصة بالشبكات، واقتحام نظم تشغيل الشبكات المختلفة، وسوق يتم تناولها بالتفصيل.

١. البحث عن المنافذ المفتوحة عن طريق الشبكات

يتطلب الاختراق المباشر الكثير من الجهد والمثابرة وتكرار المحاولة بعد المحاولة لاكتشاف المنافذ المفتوحة والدخول منها إلى الجهاز، فبعد تحديد الهدف المراد اختراقه (بريد إليكتروني، موقع على الإنترنت، شبكة محلية مرتبطة بالإنترنت) يحتاج المخترق لجمع أكبر قدر ممكن من المعلومات حول مظاهر أمن النظم الخاصة بالهدف قبل القيام بمحاولة الاختراق وتشمل عملية جمع المعلومات، أسماء الميادين، وكتل الشبكات، وعناوينIP، وخدمات TCP، وخدمات TCP/UDP، وبنية النظام، وتعداد النظام، وأسماء المستخدمين والمجموعات ومعلومات SNMP، وبروتوكولات الشبكة المستخدمة (على سبيل المثال IPX، IP، Decent، TCP/IP)، وأرقام الهواتف الرقمية، وآليات التحقق من صحة المعلومات (المجلة الإلكترونية، ١٤٢٣هـ). وكنقطة بداية يستخدم المخترق صفحة بدء الهدف بشكل جيد، لما تقدمه صفحة البدء مقدار لا بأس به من المعلومات، كسرد بعض المؤسسات إعدادت الأمن الخاصة بهم مباشرة على ملقم الإنترنت الخاص بهم، بالإضافة لبعض المواد المهمة الأخرى الأماكن والمؤسسات أو العناصر المرتبطة، كأخبار الدمج والتحصيل، وأرقام الهواتف، وأسماء المستخدمين وعناوين البريد الإلكتروني، وسياسات الأمن والخصوصية التي تشير إلى أنواع آليات الأمن الموضوعة، ارتباطات إلى ملقمات Web أخرى مرتبطة بالمؤسسة، كما إن الحصول على نسخة من الموقع، قد تسمح للمخترق بالبحث برمجياً عن البنود المهمة الأخرى وتجعل بذلك عملية جمع المعلومات أكثر فعالية. كما يمكن أن تقدم مقالات الأخبار وإصدارات الصحف وغيرها دلائل إضافية حول وضع المؤسسة ومخطط الأمن بها، وتقدم مواقع مثل www.finance.yahoo.com وwww.companysleuth.com بحراً من المعلومات لكيف يمكن تتبع شركة تعتمد على الإنترنت بشكل أساسي (Aims.net.٢٠٠٢).

كما قد يلجأ المخترق إلى استخدام عملية تعداد الشبكة في التعرف على أسماء الميادين حيث تمثل أسماء الميادين حضور المؤسسة على الإنترنت، وهي المكافئ على الإنترنت لأسم المؤسسة،

ولكي يتم تعداد هذه الميادين، يتم البدء باكتشاف الشبكات المقترنة بها، وتساعد قواعد بيانات Whois المتعددة بتقديم ثروة من المعلومات حول الجهة المستهدفة، كما يوجد هناك آليات مختلفة عديدة للاستعلام من قواعد البيانات Whois، ومن أهم هذه المصادر موقع http://www.allwhois.com/ ويقدم أنواع الاستعلامات التي يستخدمها المخترقون لبدء هجومهم كعرض معلومات التسجيل وملقمات Whois المقترنة بها (المجلة الإلكترونية، ١٤٢٣هـ).

كما تعرض عملية تعداد الشبكة كل المعلومات المتعلقة بالشبكة كعنوان (IP)، ونقطة الاتصال POC، والأشخاص المسؤولين عن النظام، وبعد التعرف على كل الميادين المقترنة يتم الاستعلام عن DNS، وهو قاعدة بيانات موزعة تستخدم لتقابل عناوين (IP) مع أسماء مضيفين والعكس بالعكس، وإذا كان DNS معد أصلاً بشكل غير آمن، فمن الممكن الحصول على معلومات مهمة حول الجهة المستهدفة. كما يتم استغلال الأخطاء التي يمكن أن يرتكبها مدير النظام بأداء عملية نقل منطقة Transfer Zone، كما أن العديد من ملقمات DNS والمعدة بشكل سيئ تقدم نسخة لأي شخص يطلبها، حيث تعطي هذه النتيجة أسماء المضيفات الداخلية وعناوين (IP) وهي الهدف الذي ينشده المخترق، لأنها بمثابة لتقديم مخطط عمل كامل أو مخطط الطريق للشبكة الداخلية في المؤسسة، وبعد الحصول على تلك المعلومات الخاصة بالهدف يحتاج الوصول إلى الهدف من الإنترنت تقنيات مسح المنافذ Scanning بدلالة جمع المعلومات (Aims.net.٢٠٠٢).

٢. استغلال المنافذ المفتوحة

عندما يتم الاتصال بالشبكات المحلية أو الدولية يصبح القرص الصلب عرضة للاختراق. ويتم باستغلال المنافذ الموجودة بالنظم أو برامج الحماية وذلك للدخول على جهاز أو شبكة حاسب آلي مرتبطة به (Grabosky, & Smith, ١٩٩٨). ومن المنافذ التي يمكن استغلالها المنافذ الموجودة في البرامج التي تعتمد نظام الزبون/الخادم Client/server أو استغلال الفجوة الأمنية ببرنامج الدردشة ICQ وهو أحد منتجات شركة Mirabils الإسرائيلية إذ يستخدم برنامج ICQ بروتوكول الزبون

للزبون Protocol Client-To-Client الذي يعطي الصلاحيات للمستخدمين باستقبال أي شيء بدون تقدير للأضرار التي قد تنجم عن ذلك مقارنة بالنظم التي تستخدم بروتوكول زبون المزود Client-Server Protocol (إنترنت العالم العربي، ١٤٢٣هـ). كما يتم استغلال المنافذ المفتوحة في نظم التشغيل والتطبيقات العاملة معه كالتطبيقات التي تعمل مع التقنيات التي تعتمد بروتوكول Telnet الذي يسمح بالوصول إلى أجهزة الحاسب آلي عن بعد وتنفيذ الأوامر عليها (Khalal٢٢, ٢٠٠٢).

وكشفت الوثيقة الصادرة من FBI والجهات ذات العلاقة في سبتمبر عام ٢٠٠١م بوجود حوالي (٢٠) منفذ في نظام التشغيل Windows Me تم استغلالها للاختراق (إنترنت العالم العربي، ١٤٢٣هـ). كما يمكن استغلال المنافذ المفتوحة في مزود الويب Web Servers مثل مزود IIS، كما يمكن النفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثور على ملفات مشاركة غير محمية، ويسهل وقت انهيار النظام أو حجبه عن الخدمة، أو وقت إعادة إقلاعه الطريق أمام المخترق، ويتم ذلك بعدة طرق وعلى مختلف النظم (العبد المحسن، ١٤٢٣هـ). كما يتم الاستفادة من تفعيل خيارات مشاركة في الملفات والطباعة File And Sharing Print الموجودة في لوحة التحكمControl Panel أثناء الاتصال بالإنترنت، واستغلال الخصائص المتوفرة في المتصفح Browser كخاصية الرجوع للخلف في المتصفح، وتذكر إسم المستخدم وكلمة المرور، والإكمال الآلي للاسم، وفراغات النماذج، كما يتم استغلال الأخطاء البشرية في البرمجة المقصودة أو غير المقصودة (المجلة الإلكترونية، ١٤٢٣هـ).

٣. كسر كلمات المرور الخاصة بالشبكات

يتم الدخول عبر منفذ بروتوكول FTP للحصول على ملف كلمات المرور ضمن الملف الخاص بأحد المشرفين على الشبكة (Khalal٢٢, ٢٠٠٢). يتم تخزين كلمات المرور مع أسماء المستخدمين والصلاحيات في ملف SAM الموجود في WINNT\System٣٢\config حيث هو الهدف الأول للمخترقين الطامحين للحصول على امتيازات معينه، حيث يقوم المخرب بالحصول على

ملفSAM، عند الإقلاع بنظام بديل باستخدام DOS أو بإنشاء قرصRepair في NT٤,٠ ويتم ذلك باستخدام الآمر Rdisk وفي Windows٢٠٠٠ من الطرفية Backup وعند إنشاء هذا القرص يتم نسخ الملف SAM، ومن ثم استخراج خلائط كلمات المرور من حساب المديرAdministrator (Nor٢٠٠٠, ٢٠٠٢). وقد يلجأ المخترقون بعد الحصول على ملف كلمة المرور إلى استخدام برامج خاصة لتخمين كلمات المرور كبرنامج Lop track (Khalal٢٢, ٢٠٠٢).

٤. اقتحام نظم تشغيل الشبكات المختلفة

تقدم بعض المؤسسات برامج تقتحم نظم تشغيل الشبكات المختلفة، بحيث تسمح بالدخول إلى المزوّدات العاملة باستخدام صلاحيات مدير الشبكة، وبدون معرفة كلمة المرور الخاصة به، مع إمكانية تغيير هذه الكلمة، وعند تغيير كلمة المرور يعمم البرنامج رسالة بشكل آلي إلى كافة الأجهزة المتصلة بالشبكة، يخبرها بتغيير كلمة سر مدير الشبكة (Nor٢٠٠٠, ٢٠٠٢).

٣-٣-٢-٢ الاختراق المبطن

باستخدام تطبيقات معينة تتجاوز الجدران النارية حيث تحمل ملفات التجسس تلقائيا عبر الإعلانات المصاحبة للمواقع أو من خلال مرفقات رسائل البريد الإلكتروني أو برامج المحادثة حيث لا يرصدها الجدار الناري وباقي برامج الحماية وتعدها من بنود بروتوكولات الاتصال. ويتبع المخترقون بعض الطرق في الاختراق المبطن، كإرسال أحصنة طروادة Trojan Horses حيث يقوم المخترق بالبحث في مجال محدد مسبقاً من عنوانين الإنترنت عن مستخدم ما، وفي حالة إيجاد الجهاز سيظهر للمخترق رقم أو عنوان الهدف، بعد ذلك لا يتبقى على المخترق إلا تحديد البرنامج الذي يتعامل معه، ولكي يستطيع اختراق جهازه يقوم بإرسال أحصنة طروادة الذي بفتح منفذ اتصال يسمح للمخترق بالدخول والتحكم بالجهاز (بوابة التكنولوجيا والاتصالات، ١٤٢٣هـ)

ويدخل تحت مسمى أحصنة طروادة Trojan Horses برامج لها عدة مسميات كبرامج الباب الخلفي Backdoor (العبد المحسن، ١٤٢٣هـ)، أو أدوات تجسس وإرسال معلومات، أو برامج التحكم من بعد، حيث تقوم بتلك المهام وأهم ما تقوم به هو جمع كل المعلومات التي يريدها المخترق ومن ثم إرسالها إلى مصدر البرنامج (مجلة الأمن الإلكترونية، ١٤٢٣هـ)، ومن تلك البرامج؛ برنامج Black Orifice وبرنامج Net Bus، وبرنامج Sub Seven والتي تثبت نفسها على النظام بالطريقة التي تتبعها الفيروسات، ويختار المخترق واحد من الأساليب لجعل الضحية يقوم بتحميل تلك البرامج كأن يضمّنها المخترق كملفات مرفقة Attachment ضمن رسالة بريد إلكتروني أو عن طريق برامج الدردشة Chatting أو وضعها في موقع إنترنت ووصفها بأنها برامج مفيدة، في محاولة لخداع زوار الصفحة لجلب هذه البرامج وتثبيتها على أجهزتهم إلى أن يحاول المخترق إجراء اتصال من خلاله، حيث يتيح للمخترق الوصول عن بعد إلى كافة أجزاء النظام (العبد المحسن، ١٤٢٣هـ). أو يطلب تحميل البرامج المجانية من مواقع على الإنترنت بإرفاق تلك البرامج المجانية بملفات تحمل برامج تجسس لتفتح منافذ في الجهاز المستهدف، ومن ثم يتم الحصول على المعلومات المخزنة بجهاز الحاسب الآلي، أو يتم تدمير تلك المعلومات، وقد يكون طلب تحميل البرامج المجانية من قبل بعض المؤسسات بهدف تجربة المنتج على أرض الواقع، واستخدام أجهزة الغير كحقل تجارب (مجلة الأمن الإليكترونية، ١٤٢٣هـ).

ويعتمد المخترقون الذين يرسلون برامج الباب الخلفي كملفات مرفقة على البريد الإلكتروني الذي يعد أكثر الأساليب استخداماً وتقوم تلك الملفات المرفقة بإعادة تحميل نظام التشغيل ومن ثم العمل في الخفاء وتقوم بإضافة نفسها في كل رسالة ترسلها دون علم المستخدم (مجلة الأمن الإلكترونية، ١٤٢٣هـ). حيث يعتقد الضحية أن برنامجاً مرفقاً باسم runme.exe هو برنامج آمن والرسالة قادمة من شخص يدعي أنه مدير الشبكة أو خبير تقني ويقدم للمستخدم هذا البرنامج على أنه برنامج لمضاعفة سرعة الاتصال بالإنترنت، أو غيرها (العبد المحسن، ١٤٢٣هـ). وغالباً لا تقوم برامج الحماية بمنع

استقبالها حيث تعدها نوع من أنواع برتوكولات الاتصالات ولكن عند تشغيل برنامج الحماية يقوم باكتشاف تلك البرنامج وتعامل معه. وتنفذ تلك البرامج المرفقة حتى لو كان هناك جدران نارية وبرامج حماية وذلك لقدرة هذا النوع من استغلال نقاط الضعف في معظم أنواع الجدران النارية التي تسمح بخروج وتصدير المعلومات من الجهاز أو الشبكة المحلية بواسطة FTP And HTTP (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

كما يقوم بعض المخترقين بإرسال برمجيات جافا Java Applets أو تحكمات Java Active أو Java x والتي تقوم باصطياد المعلومات لأنها قادرة على رصد كلمات المرور، وكذلك تدمير وتعديل الملفات المخزنة أو ملفات البرامج، وقد تؤدي إلى تخريب نظام التشغيل (مجلة الأمن الإليكترونية، ١٤٢٣هـ). وقد يعمد بعض مدراء المواقع بتصميم برنامجاً صغيراً، كتصميم برنامج بلغة جافا Java ويضمنه أوامر التجسس التي يريدها، ويضعه على إحدى صفحات موقعه، ويجعله على شكل معين، فقد يكون صورة متحركة، أو إعلاناً، أو عدد الزيارات، أو سجل الزوار، أو مجرد إعلان صغير، وعندما يأتي الزائر لطلب الصفحة عبر المتصفح يعمل البرنامج على حاسبه كأنه الذي قام بتشغيله، فيجمع المعلومات المطلوبة، ويرسلها عبر الوصلة المفتوحة مع الإنترنت إلى الموقع الذي يخزن المعلومات، وتتم هذه العملية بسرعة فائقة، وبدون أن يشعر بها الزائر، كما يمكن ببساطة طمس كل أثر لها (الإيهم، ١٤٢٣هـ).

٣-٣-٢-٣ استغلال المعلومات التي يقدمها برنامج التصفح

يتم استغلال Cookie في جمع معلومات عن المستخدمين خلال تصفحهم للمواقع، فعن طريقه يتم معرفة عنوان (IP) الذي يميزه عن غيره، فعندما يتم طلب صفحة من موقع على الإنترنت، يقوم البرنامج المستخدم للتصفح بتزويد الموقع بعنوان (IP)، وبشكل أساسي يقدم المتصفح إلى مزود الخدمة مجموعة من المعلومات التي يمكن أن تعد ضرورية لعمل الشبكة، أهمها التعريف عن المتصفح نفسه، كنوع المتصفح، ورقم إصداره، ودقة الشاشة التي يعمل عليها، والعمق اللوني

المستخدم. وبعض المتصفحات تقدم أيضاً اللغات على الحاسب، وبعض المتصفحات الحديثة ترسل عنوان الصفحة السابقة إلى مزود الخدمة، وهذه عملية تجسس حقيقية، لأن هذه الميزة الجديدة أضيفت إلى الأجيال الجديدة من المتصفحات بناء على طلب مدراء المواقع، لتسمح بمراقبة حركة الزوار بين المواقع على الشبكة، بالإضافة إلى هذه المعلومات، يستطيع مدير أي مواقع مراقبة حركة الزائر ضمن موقعه، ويربط هذه الحركة برقم التعريف (IP) ونشاطه على الموقع، فتتشكل لديه قاعدة بيانات حقيقية عن الزائر تحوي معلومات قيمة يمكن الاستفادة منها لتطوير الموقع أو تستغل لأغراض أخرى (الإيهم، ١٤٢٣هـ).

ويمكن جمع معلومات عن الزوار كإسم البلد واللغة والوقت، وعن الصفحات الأكثر طلباً من قبل الزوار القادمين من بلد معين، بالإضافة إلى أنواع أخرى من المعلومات. وكل هذا بدون أن يشعر به الزائر، ودون أن يظهر شيء على شاشته. وأي مدير موقع يمكن أن يستخدم هذه البيانات في دراسة ميول وانطباعات زوار الموقع، وهي معلومات شخصية لا تتعلق بالموقع، بل بالزوار ويبدو الوضع أخطر إذا صمم الموقع أصلا لاختبار طرق التأثير على الرأي العام، ولإيصال رسائل سياسية أو اجتماعية إلى أناس محددين على الإنترنت (الإيهم، ١٤٢٣هـ).

وإذا استخدمت هذه التقنيات على موقع من مواقع التجارة الإلكترونية، يمكن أن تعكس الوضع الاقتصادي للزائر، عبر معرفة المواضيع التي يزورها والتي يهملها. ويمكن أن يكون هناك استخدامات أخرى لهذه التقنية، خصوصاً إذا اشترت المعلومات جهات تعرف كيف تستفيد منها، كما أن مدراء المواقع يستطيعون الحصول على كمية كبيرة من المعلومات عن الزائر بشكل طبيعي اعتماداً على ما يرسله لهم المتصفح من معلومات، أي ما يرسله عند اتصاله بالموقع للحصول على الصفحة التي يطلبها. وهم لا يحتاجون إلى أية أدوات معقدة، ولا إلى إرسال برامج خاصة تعمل على الحاسب الآلي وتبث إليهم معلومات. ولا يستطيع الزائر فعل أي شيء في المقابل إلا إذا قرر عدم زيارة الموقع نهائياً (الإيهم، ١٤٢٣هـ).

٣-٣-٢-٤ كسر كلمات المرور في أجهزة الحاسب الآلي passwords crack

أدى نسيان كلمات المرور إلى الحاجة إلى وسيلة لكسر كلمات المرور والوصول إلى المعلومات المطلوبة، ولذلك ظهرت العديد من البرمجيات التي تساعد على كسر كلمات سر الملفات المحمية أو تكشف كلمة سر حافظ الشاشة أو كلمة سر مدير الشبكة. ومثلما تساعد هذه البرمجيات على استعادة كلمات المرور المنسية أو تخفيف الأضرار في حال تعمد إغلاق الملفات بكلمات مرور، فقد يساء استخدامها وتوظف في أعمال إجرامية كالدخول إلى شبكات الإدارات الحكومية والمؤسسات والمصارف والتلاعب بالمعلومات أو إلغائها أو تحويل الأموال بين الحسابات بطريقة غير شرعية، وكشف كلمات المرور لا ينتهي فمؤسسات تطوير التطبيقات تسعى دائماً إلى رفع مستوى أمن تطبيقاتها، بحيث يصبح كسر حماية ملفاتها في الإصدارات الجديدة، أكثر صعوبة عما كان عليه مع ملفات الإصدارات الأقدم، وتقابلها مؤسسات كسر الحماية بابتكار طرق وأدوات اختراق جديدة بعد فترة (إنترنت العالم العربي، ١٤٢٣هـ).

٣-٣-٢-٦ رصد لوحة المفاتيح

من أخطر مصادر التهديد الأمني. حيث أن المجرمين قادرون على رصد أي ضغطة على لوحة المفاتيح وبذلك يتمكنون من رصد كل ما يتم كتابته على لوحة المفاتيح خاصة إسم المستخدم وكلمات العبور وذلك حتى قبل أن يتمكن الجهاز أو برنامج من إخفاء وتشفير الكلمة. ولحسن الحظ فإن هذه البرامج غير منتشرة عبر الشبكة لأنها تتطلب الوصول إلى الجهاز فعلياً, يستخدمها مجرمي نظم المعلومات لرصد معلومات عبر مقاهي الإنترنت، والأجهزة العامة في المكتبات، وغيرها من الأماكن، حيث يتردد الكثير من المستخدمين ممن يعتمدون على الأجهزة العامة كمقاهي الإنترنت ولا يمتلكون أجهزة خاصة بهم للشراء المباشر من الإنترنت واستخدام بطاقات الائتمان أو التحويل البنكي (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

٣-٣-٢-٨ IP Spoofing

هو مصطلح يطلق على عملية انتحال شخصية للدخول إلى عناوين للمُرسِل والمُرسَل إليه. وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة ومن خلال طريقة تعرف بمسارات المصدر Source Routing فإن حزم (IP) قد يتم إعطائها شكلاً تبدو معه وكأنها قادمة من حاسبات آلية معينة، بينما هي في الحقيقة ليست قادمة منه، وعلى ذلك فإن النظام إذا وثق ببساطة بالهوية التي يحملها عنوان مصدر الحزمة فإنه يكون بذلك قد خدع، والبريد الإلكتروني يمكن أيضاً أن يخدع بسهولة ولكن النظام المؤمن بشكل جيد لا يثق بهذه المصادر ولا يسمح بالحركة المسيّرة من قبل المصدر Source Routed (الهاجري، ١٤٢٢هـ).

٣-٣-٣ أدوات ارتكابها

تم حصر مجموعة من الأدوات التي تستخدم لارتكاب جرائم نظم المعلومات، كأدوات اختراق الشبكات وأجهزة الحاسب الآلي المرتبطة، وأدوات إغراق البريد الإلكتروني، وأدوات تعطيل الأجهزة والمواقع، وأدوات تدمير الملفات وقواعد البيانات، وأدوات كسر كلمات المرور في أجهزة الحاسب الآلي، وبالتفصيل على النحو التالي:

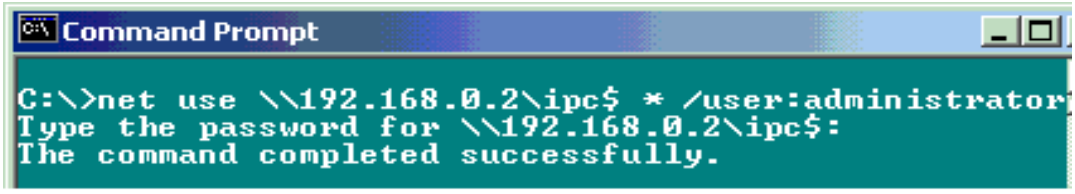
٣-٣-٣-١ أدوات الاختراق المباشر للشبكات وأجهزة الحاسب الآلي المرتبطة

١. تقنيات مسح المنافذ: هي أدوات تستخدم لفحص الشبكات والمراقبة ولكن يمكن أن تستغل تلك المنافذ التي تم تحديدها للقيام بإصلاحها أن يخترق منها كتقنية Super Scan والتي يتم الحصول عليها من Http://Keir.Net/Software.Html وهي إحدى أكثر ماسحات منافذ TCP سرعة ومرونة، وتقنية Winscan ويمكن تنزيلها مباشرة من موقع Http://Www.Prosolve.Com وهي ماسح منافذ TCP ويستخدم عادة في إصدار سطر الأوامر للنصوص البرمجية لقدرته على مسح شبكات من حجم C، وتقنية Wups ماسح خاص للمنافذ

UPS إلا إنـه يمسـح مضـيف واحـد مـن أجـل منافـذ محـدده ويـتم الحصـول عليـه مـن Http://Ntsecurity.Nu، وتقنية Pinger ماسح فردي لبيئة نظام تشغيل windows ويتم الحصول عليها من موقع Ftp://Ftp.Technotronic.Com/Rhino٩-Products/Pinger.Zip ، كما تتوفر عـدة أدوات للمسـح بموقـع Zd.net ويـتم تحميـل هـذه التقنيـة مـن الموقـع Http://Www.Zdnet.Com/Downloads/Stories/Info/٠,,٦٨٩٨١,.Html ومـن أشـهرها Port scan الخـاص برصـد المنافـذ المفتوحـة علـى الأجهـزة الشخصـية المربوطـة بالشـبكات (Aims, ٢٠٠٢).

٢. أدوات كسـر كلمـات المـرور بالشـبكات: كـأداة Pwdump مـع NT٤,٠ و pwdump٢ مع٢٠٠٠Windows وبرنامج Lop track للاستخراج كلمات المرور من ملفات الشبكات، ويمكن الحصول عليها من www.nor٢٠٠٠.com/pwdump٢.zip، أو برنامج تخمين كلمات المرور من خلال الشبكة، وفي حالة استخدامه واصطياد كلمة المرور تبين العبارة التالية (لقد وصلت لكلمة المرور الخاصة بالمدير تهانينا، أنت الآن المدير بقوة القانون)، كما يظهر البرنامج نجاح العملية (Nor٢٠٠٠, ٢٠٠٢)، كما في شكل رقم (٤).

شكل رقم (٤) صورة من برنامج تخمين كلمات المرور من خلال الشبكة



المصدر: (Nor٢٠٠٠, ٢٠٠٢)

٣. استخدام برامج خاصة لتخمين كلمات المرور بالشبكات من أكثر هذه البرامج انتشار Cracker Jack، وJohn The Ripper، وJack The Ripper، وBrute Force Cracker، وتعمل

هذه البرامج على جميع الاحتمالات الممكنة لكلمة المرور، من حروف وأرقام ورموز لكنها تستغرق وقتاً أطول في التوصل إلى هذه الكلمة، إذا احتوت على عدد أكبر من الرموز وقد تصل الفترة التي تتطلبها هذه البرامج للتوصل إلى كلمة المرور إلى سنوات بناءً على عدد الرموز المستخدمة والنظام المستخدم في عمليات التخمين (Khalal٢٢, ٢٠٠٢).

٤. أدوات اقتحام نظم تشغيل الشبكات المختلفة كبرنامج Net Ware Access Utility، وبرنامج Net Access Utility، وبرنامج Crack٥ الذي يعمل في بيئة نظام التشغيل Unix، وبرنامج Lop Track الذي يعمل في بيئة Windows ويمكن الحصول على تلك البرنامج من موقع www.nor٢٠٠٠.com/Lophtcrack..htm (Nor٢٠٠٠, ٢٠٠٢).

٢.٣.٣.٣ أدوات الاختراق المبطن

١. برنامج Net Bus

تمكن مبرمج عام ١٩٩٨م سويدي كارل نيكتر من إصدار نسخة تعمل على Windows ٩٥ من برنامج لم يطلق عليه إسم في ذلك الوقت يستطيع مستخدم البرنامج تشغيله بواسطة حاسب آلي بعيد يسمى أتوبيس الشبكة صدرت بعد ذلك نسخ عديدة منها Net Bus Pro وNet Bus ٠٠٠٢ (حسام الدين، ١٤٢٣هـ). يتميز بسهولة استخدامه وانتشار ملف التجسس الخاص به في كثير من الأجهزة مما يجعل الاختراق به سهل للغاية (Nanoart, ٢٠٠٢). ويسمح البرنامج لأي شخص بالسيطرة على جهاز الضحية عن بعد بعرض صورة مفاجئة على شاشة أو تغيير إعدادات الشاشة أو إعدادات النظام دون تدخل من المستخدم كفتح وغلق CD Driver تلقائياً، ووضع مؤشر الفأرة في مكان معين بحيث لا يمكن للمستخدم تحريكه عن هذه المنطقة، وإلغاء Disable عمل مفاتيح معينه من لوحة المفاتيح، ويستطيع المخترق التجسس على المستخدم ورؤية كل ما يفعله. وعرض محتويات القرص الصلب بالكامل، وإنزال أو حذف أو تحميل أي

ملف من جهاز الضحية، كما يستطيع تغيير كلمات المرور، وفي حالة ارتباط ميكروفون بجهاز الضحية يمكن للمخترق الاستماع لما يدور من حديث (العبد المحسن، ١٤٢٣هـ).

٢. برنامج Black Orifice

يسمى الفجوة السوداء. وهو ثاني أشهر برامج الاختراق وأقدمها وأبرز إصدارته السابقة يحمل النسخة رقم ١,٢ وقد أصدرت الجمعية التي تصدره وأسمها "جمعية البقرة الميتة Cult of Death Cow بإنتاج نسخة جديدة منه Black Orifice ٢٠٠٠، يقوم البرنامج بسيطرة الكاملة على جهاز الضحية وتظهر نفس أعراض برنامج Net Bus (العبد المحسن، ١٤٢٣هـ).

٣. برنامج Sub Seven

من اشهر البرامج المستخدمة بالمنطقة العربية ويفضل لوجود نسخة بالغة العربية منه وأيضاً لبساطته وسهولة تعلمه وسهولة الاختراق عن طريقة، يتميز بمخادعة الشخص الذي يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفه من ملف التسجيل Windows وأعراض الإصابة بهذا البرنامج تظهر رسالة (قام هذا البرنامج بإنجاز عملية غير شرعيه ....) عند كل مرة يدخل فيها المخترق لجهاز الضحية ويستطيع المخترق التجسس على المستخدم ورؤية كل ما يفعله (العبد المحسن، ١٤٢٣هـ).

٤. أدوات اختراق أخرى

يوجد عدد من البرامج التي يمكن استخدامها في الاختراق وتأتي بالمرتبة الثانية بعد البرامج الثلاثة الشهيرة (Net Bus، Black Orifice، Sub Seven). وهي (مرتبة حسب خطورتها) Hack a Tack، Master Paradise، Deep Throat، Girl Friend، Sphere، Win Crash، Big Cluck، Executer (العبد المحسن، ١٤٢٣هـ). كما يتم استخدام أدوات اختراق وهي متداولة عربياً، وأحد الطرق المتبعة للحصول عليها هي الإنترنت مثل Muter, Win Nuke,

Arabic) Assault, Lorwna, Mirror ٢١, Wet State, Jojoba, Lcmp, Muerte , Knew, Deviant hackers, ٢٠٠٢).

٥. Cookie

عبارة عن ملفات نصية، فهي ليست برامج أو شفرات برمجية، ويهدف هذا Cookie إلى جمع بعض المعلومات، وهو مفيد أحياناً، خاصة إذا كان الموقع يطلب إدخال كلمة مرور، ففي هذه الحالة لن يطلب كلمة مرور في كل زيارة، إذ سيتمكن الموقع من اكتشافها بنفسه عن طريق Cookie الذي تم وضعه على القرص الصلب في الزيارة الأولى، أي تحتوي هذه الملفات النصية Cookie على معلومات تتيح للموقع الذي أودعها أن يسترجعها عند أي الزيارة مقبلة للموقع، وعند إدخال عنوان موقع في شريط العناوين يرسل المتصفح طلباً إلى الموقع الذي حدده متضمناً عنوان (IP) الخاص به، ونوع المتصفح الذي يستخدمه، ونظام التشغيل، تخزّن هذه المعلومات في ملفات خاصة بالمزود Log Files، وفي الوقت نفسه، يبحث المتصفح عن ملفات Cookie التي تخص الموقع المطلوب، فإذا وجدها يتم إرسالها مع طلب مشاهدة الموقع، وإذا لم يجدها لا يتم إرسال أي معلومات (الإيهم، ١٤٢٣هـ).

يستطيع الموقع عند استلامه طلب المشاهدة مع ملف Cookie أن يستخدم المعلومات الموجودة في الملف لأغراض مختلفة، وأن لم يجد ملف Cookie، فإن الموقع سيدرك أن هذه الزيارة الأولى إليه، أو أن تاريخ الصلاحية قد انتهاء، فيقوم بإرسال ملفات Cookie إلى الجهاز ليخزنه علية. وبإمكان الموقع تغيير المعلومات الموجودة ضمن ملفات Cookie أو إضافة معلومات جديدة كلما تمت زيارة الموقع، وتساعد تلك المعلومات المخترقين في الوصول إلى أهدافهم (صلاح، ٢٠٠١م).

٦. **Java Active**

لغة برمجة كائنيه Object-Oriented طورتها شركة Sun Microsystems تستخدم لإضافة الرسوم المتحركة، وأسعار البورصة الفورية، وغيرها من المزايا الديناميكية إلى صفحات Web. ويمكن إرسالها من المزود Server إلى المتصفح، الذي يستطيع فك شيفرتها وتنفيذها، بواسطة ما يسمى آلة جافا الافتراضية JAVA Virtual Machine (JVM) . حيث توفر معظم برامج التصفح شائعة الاستخدام الدعم للغة جافا (إنترنت العام العربي، ١٤٢٣هـ).

٧. **JavaScript**

لغة طورتها كل من شركتي Sun Microsystems وNetscape لتسهيل إضافة مزايا تفاعلية إلى صفحات Web. وعلى الرغم من كونها مشتقة من لغة جافا، فإن جافاسكريبت تمثل لغة منفصلة. وتنحصر فاعلية جافاسكريبت في جهة الزبون Client حيث أن المفسر Interpreter الذي ينفذ تعليماتها، يكون مدمجاً في المتصفح (إنترنت العام العربي، ١٤٢٣هـ).

٨. **ActiveX**

اسم تطلقه مايكروسوفت على مجموعة تقنياتها Object-Oriented التي تهدف إلى تحقيق إمكانية إدخال مزايا ديناميكية إلى صفحات Web. لا تحظى لغة ActiveX حالياً إلا بدعم عدد محدود من المطورين، بالإضافة إلى منتجات مايكروسوفت المرتبطة بإنترنت مثل برنامج التصفح Internet Explorer، ولكن مايكروسوفت تعد ActiveX جزءاً أساسياً من استراتيجيتها (إنترنت العام العربي، ١٤٢٣هـ).

٣-٣-٣-٣ البريد الإلكتروني وبرامج المحادثة

يتم استخدام تلك الأدوات كوسيلة لنقل الفيروسات، والديدان الإنترنت، وبرامج الاختراق وغيرها وذلك بإرفاق بالرسائل الإلكترونية ملفات تنتهي باختصار مثل Executable =(EXE) Files ويعني وجود ملف تنفيذي أو Command Files = (COM) ويعني وجود ملف به أوامر

للتنفيذ مرتبطة بأي جزء من الملف وتبدأ بالعمل بعد مرور وقت معين أو حين الضغط على جزء معين، أما اختصار Batch File = (BAT) يعني وجود أمر معين موجه لأحد ملفات نظام التشغيل، وأما اختصار Application = (APP) ويعني وجود ملف به برنامج تطبيقي وهو أحد برامج التجسس (مجلة الأمن الإلكترونية، ٢٠٠٢م).

٣-٣-٣-٤ أدوات إغراق البريد الإلكتروني

يتم استخدام برامج جاهزة خاصة للإغراق Flooding ومتوفر بكثرة على الإنترنت، كبرامج Bomb، وAvalanche، وEuthan، وQuickfyr، والمتوفرة على موقع www.arabichackers.com (Arabic hackers, ٢٠٠٢). بالإضافة إلى إمكانية استخدام برنامج ICQ للإغراق (Aims, ٢٠٠٢).

٣-٣-٣-٥ أدوات تعطيل الأجهزة والمواقع

من أشهر أدوات تعطيل الأجهزة والمواقع DDOS (Distributed Denial Of Service) برامج TRINOO، وTribe Flood Net، وTFN٢K، و Stacheldraht. استخدماً في الهجوم على كبرى مواقع إنترنت، مثل Zdnet وYahoo وEmbay، وAmazon، وCNN، وغيرها استغلالها لتدمير الموقع. مما يمكن أن يشكل خطراً على شبكة إنترنت كلها، وليس على بعض المواقع فقط، حيث أن كل موقع من المواقع التي أصيبت، بهذا النوع من هجمات حجب الخدمة، تم حجز جزءاً كبيراً من حزمة البيانات في الإنترنت، ما قد يهدد الشبكة بالكامل، وأن حدث ذلك يوماً، فيتوقع أن يشهد العالم أزمة اقتصادية شاملة (khalal٢٢, ٢٠٠٢).

٣-٣-٣-٦ أدوات تدمير الملفات وقواعد البيانات

١. الفيروسات

برامج صغيرة تصيب الأجهزة وتتسبب في الكثير من المشاكل كمسح الذاكرة الصلبة أو مسح بعض الملفات الهامة في نظم التشغيل أو القيام بإصدار الأوامر لبعض البرامج بدون تدخل مباشر، هو برنامج يكرر نفسه على نظام الحاسب آلي عن طريق دمج نفسه في البرامج

الأخرى، لم تكن الإنترنت الوسيلة الأكثر استخداماً في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات.

٢. دودة الإنترنت

تسبب بالضرر المباشر للملفات والبرامج والبيانات الموجودة على القرص الصلب في الجهاز، حيث تقوم أحيانًا بنسخ نفسها بأعداد ضخمة، وتنجح في إيقاف وتعطيل النظام، وتكمن خطورة دودة الإنترنت Internet Worm في قدرتها الفائقة على الخداع والمراوغة بحيث تكون عملية اكتشافها صعبة للغاية. ولديها القدرة على نسخ وتوزيع نفسها إلى النظام المعلوماتي بأكمله, وهي لا تحتاج إلى برنامج حاضن، وبإمكانها أن تتنقل بشكل مستقل خلال الشبكات وتتكاثر وتنتشر بسهولة، ويمكن أن ترسل دودة الإنترنت Worm عادة عبر البريد الإلكتروني، حيث يمكنه أن تكون على شكل رسالة لطيفة أو لعبة، وعلى سبيل المثال دودة Melissa استعملت فهرس عناوين صندوق البريد الإلكتروني، لإرسال نفسها كرسالة إلكترونية من صديق، وبناءاً على ذلك وثق المستلمون في الرسالة، وقاموا بفتح الرسالة الملحقة بالبريد الإلكتروني. وأيضاً الدودة الحمراء التي استطاعت خلال أقل من تسع ساعات اقتحام ما يقرب من ربع مليون جهاز في (١٩) يوليو ٢٠٠١م (مجلة الأمن الإلكترونية، ٢٠٠٢م).

٣-٣-٣-٧ أدوات كسر كلمات المرور في أجهزة الحاسب الآلي

التسابق بين مؤسسات تطوير التطبيقات وبين مؤسسات تقديم أدوات كسر الحماية وكشف كلمات المرور لا ينتهي. فمؤسسات تطوير التطبيقات تسعى دائماً إلى رفع مستوى أمن تطبيقاتها، بحيث يصبح كسر حماية ملفاتها في الإصدارات الجديدة، أكثر صعوبة عما كان عليه مع ملفات الإصدارات الأقدم، وتقابلها مؤسسات كسر الحماية بابتكار طرق وأدوات اختراق جديدة، بعد فترة. توفر مؤسسات التقنية مثل شركة Access Data Corporation وشركة Crack Software والشركة، Professional Help برامج كسر كلمات المرور Passwords Crack التي

تراوح بين كسر كلمات مرور ملفات وبرامج معالجة الكلمات والجداول الممتدة، وكلمات مرور حافظ الشاشة في الأجهزة الشخصية وبرامج توليد أرقام ومعلومات البطاقات الائتمانية إلى برامج الدخول إلى جميع نظم الشبكات، ومن بين أدوات كسر كلمات المرور مجموعة تدعى Password Recovery Modules التي تسترجع كلمات المرور إن كانت مؤلفة من عشرة أحرف سواءً كانت هذه الكلمات مكتوبة باللاتينية أو بالعربية أو كانت مختلطة عربية ولاتينية، وتتعامل كل وحدة برمجية، مع ملفات البيانات المشكلة بواسطة أحد التطبيقات فتكشف كلمات المرور للملفات ذات مستويات الحماية المتعددة، مثل كلمات المرور الخاصة بكل ورقة عمل في ملفات Excel أو كلمات المرور ذات صلاحيات الوصول المختلف في ملفات Word مهما كان طول كلمات المرور (إنترنت العالم العربي، ١٤٢٣هـ).

تتكون هذه المجموعة من Password Recovery Toolkit، WD Crack و MS Word Cracker، وEx Crack، وMS Excel Cracker، وأما برنامج Crack Sure، فإنه يعمل في خلفية Background نظام التشغيل ويسجل كلمات المرور المستخدمة لحفظ ملفات التطبيقات. أما برنامج Revelation ينحصر في كشف كلمات المرور المخزنة في نظام، والتي تعرضها على الشاشة كرموز، فإذا (مثلاً) استخدم الاتصال الشبكي الهاتفي، وتم وضع إشارة تحديد إلى جوار الحقل "حفظ كلمة المرور" بعد كتابة كلمة المرور في الحقل المخصص لها، فلا يلزم إعادة كتابة كلمة المرور في المرات القادمة لأنها ستظهر كسلسلة من رموز النجمة ويكفي تركيب برنامج Revelation وتشغيله ثم نقر بزر الفأرة فوق أيقونة الدائرة التي تحتوي خطين متعامدين في نافذة Revelation وتسحب إلى حقل كلمة المرور في نافذة الاتصال فتظهر كلمة المرور في الحقل المخصص لها في نافذة Revelation، ومن ثم يظهر الرقم السري مكتوباً وليس على شكل رموز (إنترنت العالم العربي، ١٤٢٣هـ).

٤.٣.٣ خصائصها

إن الجرائم التي تقع من خلال نظم المعلومات في أكثر صورها مستترة وخفية، لا يلاحظها المجني عليه غالباً أو يعرف بوقوعها (بحر، ١٤٢٠هـ: ٤٤). نتيجة استخدام التقنية لارتكاب جرائم نظم المعلومات فإن التقنية هي التي غالباً ما تكشف الجريمة كبرامج كشف الفيروسات وأحصنة طروادة، وقد تكون جريمة اختراق بداعي التجسس لا يكون أثراً للجريمة. ويرتبط تطور أساليب جرائم نظم المعلومات بالتطور التقني السريع الذي وفر وسهل تبادل المعلومات عن طريق وسائل اتصالات سريعة، أبرزها شبكة الإنترنت الفعالة التي ربطت العالم ببعضه وأصبح من السهولة تبادل الأفكار والخبرات والمهارات وتعلم أساليب وأدوات ارتكاب الجرائم. ويساعد ظهور شبكة الإنترنت انتشار جرائم نظم المعلومات فقد زادت أساليب إساءة استخدام تلك الشبكة في استخدامها لارتكاب بعض الجرائم، وفي ذلك تطويع لهذه التقنية لرغبات بعض المجرمين (أبو شامة، ١٤٢٠هـ : ٢٩).

أضحت جرائم نظم المعلومات مشكلة عالمية لا تعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، وصار ساحتها العالم أجمع (البداينة، ١٩٩٨م: ١٣). وقد يقوم مجرم نظم المعلومات بالابتزاز لشركة ما، أو سرقة كم هائل من الأموال، أو من المعلومات ونشرها عن طريق الإنترنت، وقد تستغل من قبل مجرمين آخرين. كاقتحام أحد المخترقين قاعدة بيانات لصفحة خاصة بالبطاقات الائتمانية على الإنترنت, وهي صفحة creditcards.com, حيث قام بتسريب أكثر من (٥٥,٠٠٠) رقم لبطاقة ائتمانية كانت محفوظة على قاعدة البيانات الخاصة بالصفحة, ثم نشر الأرقام على الشبكة بعد أن رفضت الشركة المتضررة الرضوخ لمطالبه المادية (السامرائي، ١٤٢١هـ: ١٢).

وانتقلت بعض نشاطات عدد من الجرائم التقليدية كالتجسس بالوسائل التقليدية إلى استخدام نظم المعلومات والقيام بارتكابها عن بعد، وتساعد نظم المعلومات المجرم في تسهيل ارتكاب

الجرائم التقليدية من قتل وسرقة وتزوير وغيرها من الجرائم التقليدية، لذا جعلت هناك أساليب جديدة لارتكاب الجرائم التقليدية، بحيث تتم بدون أي عناء أو استخدام للعنف. أو نقل المعلومات بين المجرمين لتفاهم حول تنفيذ جريمة تقليدية.

ومما يميز ارتكاب الجرائم بواسطة نظم المعلومات إن الشخص لا يجد حرجاً في عمل أو قول أي شئ يرغبه تجاه أفراد لا يعرفونه ولا يرونه، ويشعر أن الطرف الأخر كأنهم شخصيات في لعبة ضمن الحاسب الآلي، ويتجاهل حقيقة أن الأشخاص على الطرف الأخر يمكن أن يسبب لهم أذى أو العكس، ولذلك من سهل قيام أفراد بجرائم نظم المعلومات ولا يعتبرونها حقيقية بالنسبة لهم (المجلة الإلكترونية، ١٤٢٣هـ). تتميز جرائم نظم المعلومات عن الجرائم التقليدية بأنها ترتكب من قبل متخصصين بالحاسب الآلي كالمبرمجين، ومهندسي الشبكات ومدراءها، ومبرمجي قواعد البيانات ومدراءها، ومصممي النظام ومدخلي البيانات ومعالجيها، كما تتميز بعدم محدودية النطاق المكاني فبالإمكان سرقة بنك من واشنطن من قبل شخص يعيش في موسكو، كما يمكن ارتكاب الجريمة من المنزل دون الانتقال إلى مكان الجريمة (الشدي، ١٤٢١هـ: ٢٤٤). ويتم تنفيذ الجريمة بسرعة عالية فقد تكون مدة الجريمة جزء من الثاني، كما أنها ترتكب من قبل صغار السن والذين لا يخافون من فقدان وظائفهم، وقد ترتكب بعدد كبير من الأشخاص في نفس اللحظة.

٣-٣-٥ أصناف مجرمي نظم المعلومات

تتعدد تصنيفات مجرمي نظم المعلومات، فيمكن أن يتم تصنيف مجرمي نظم المعلومات بحسب الأعمال التي يقومون بها والأدوات التي يستخدمونها إلى المخترقون المحترفون Hackers سواء كانوا هواة حاذقين أم تقنيين مهرة، والبارعين بمجال أسلوب عمل نظم المعلومات، وخصوصاً شبكاته، والذين تبرز لديهم المقدرة على اكتشاف الأخطاء والمنافذ البرمجية والوصول إلى معلومات ما وغالباً يهدفون أما إلى إبراز قدراتهم أو يريدون الوصول إلى معلومات دون تخريب. وهؤلاء يختلفون عن الذين يهدفون إلى معرفة المنافذ بالمؤسسات حتى يتم تلافي تلك المنافذ ويكون تحت

إشراف الجهة التي تملك النظم. والصنف الثاني المخربون Crackers البارعين في اختراق النظام المعلوماتي عبر الشبكات أو أجهزته متجاوزين كلمات المرور، وبرامج الحماية الأمنية، بهدف تدمير المعلومات أو تعطيل الأجهزة والمواقع أو التلاعب في محتويات النظام المعلوماتي، والصنف الثالث المخترقون الهواة الذين يملكون الحد الأدنى من المعرفة التقنية في مجال الحاسب الآلي والشبكات، ويستخدمون مجموعة من البرامج أو النصوص البرمجية الجاهزة، ويزرون مواقع على الإنترنت بحثاً عن المزودات التي تتضمن ثغرة معينة ودخول من خلالها على النظام المعلوماتي، ويطلق عليهم المخترقون الحقيقيون مصطلح أطفال النصوص البرمجية Script kiddies (عجيب، ١٤٢٣هـ).

ويمكن تصنيف مجرمي نظم المعلومات على حسب أهدافهم إلى شخص يعمل بمفرده أو يكون ضمن منظومة بغض النظر عن هذه المنظومة فقد تكون تجارية أو سياسية أو عسكرية، ويكون خطيراً عندما يعمل داخل الجهة المستهدفة، وتكمن خطورة هذا الشخص في قدرته على معرفة معلومات حساسة وخطيرة كونه يعمل داخل تلك الجهة، لذلك فإن حرب التجسس بين الدول التي تعتمد على عناصر يعملون داخل الجهة الأخرى تعد من أخطر أنواع التجسس حيث تفرض الدول أشد الأحكام صرامة على من يمارس ذلك، والتي تصل إلى حد الإعدام في كثير من الدول. ولا يقتصر هذا الصنف على الممارسات بين الدول بل قد يكون ذلك الشخص يعمل داخل شركة حيث يقوم بسرقة معلومات تجارية سرية من تلك الشركة وذلك لغرض إفشاءها أو بيعها لمؤسسات منافسة أو التلاعب بالسجلات المالية لتحقيق أهداف عامة أو خاصة، والصنف الثاني الذين يسعون لسرقة معلومات حساسة من جهات تجارية أو حكومية وذلك لغرض بيعها على جهات أخرى تهمها تلك المعلومات والصنف الثالث لا يهدفون إلا للمغامرة وإظهار القدرات أمام الأقران، أو حب الاستطلاع، فلا توجد عادةً عند هؤلاء أطماع مالية، والصنف الرابع تلك الجهات المتنافسة التي يسعى بعضها للوصول إلى معلومات حساسة لدى الطرف الآخر، وذلك سعياً للوصول إلى

موقف أفضل من الجهة المنافسة، والصنف الخامس حكومات بعض الدول، التي تسعى من خلال حروب جاسوسية إلى الحصول على معلومات إستراتيجية وعسكرية عن الدول الأخرى، ولعل من أشهر تلك الحروب الجاسوسية تاريخياً تلك التي كانت بين الولايات المتحدة و الاتحاد السوفييتي خلال الحرب الباردة (الهاجري، ١٤٢٣هـ).

٦.٣.٣ أسباب انتشارها

أدى تنافس المؤسسات المنتجة للتجهيزات والبرامج بتوفيرها لكم هائل من المنتجات، التي تقوم بتنويع أساليب البيع، وتبسيط إجراءات التعامل مع تقنيات الحاسب الآلي (عيد، ١٤١٩هـ). كما أدى إلى توفير الإرشادات وبرامج التعليم الجاهزة، وانتشار معاهد تدريس الحاسب الآلي والإنترنت ومنح شهادات دولية من قبل المؤسسات المنتجة بقصد الدعم لمنتجاتها. وظهور شبكة الإنترنت ساعد في نشر المعلومات وتسّهيل تبادلها وتبادل الأفكار والخبرات والمهارات وتعلم أساليب وأدوات ارتكاب الجرائم، ما نظراً لما تحتويه من مواقع للمؤسسات المنتجة لها، والوسيطة، والتي تعمل روابط تشعبية وبوابات، واستضافة المواقع لتسهل الوصول لتلك الأدوات. وتقوم كثير من المؤسسات بإنتاج برامج الحماية وأدوات ارتكاب الجريمة المعلوماتية لإجبار المؤسسات بطريقة غير مباشرة على شراء أدوات الحماية بدواعي الكسب المادي، أو التحديث المستمر والمدفوع.

كما أدى نقص خبرة الأجهزة الأمنية في اكتشاف مرتكبي جرائم نظم المعلومات، وعدم الاستناد إلى وسائل تساعدهم في التحقيق في الجرائم لضبط مرتكبها، وعدم وجود تشريع شامل وواضح لكل جرائم نظم المعلومات لينطلق منه رجال القانون في مطاردة المجرمين أدى انتشار الجريمة المعلوماتية. ومما ساهم في ذلك عدم اعتبار جرائم نظم المعلومات من قبل بعض المسؤولين سواء من رجال القانون أو المؤسسات من الجرائم الخطيرة، وسهولة ارتكاب الجرائم عن بعد مما يوفر للمجرم الإحساس بالأمان والشعور بعدم كشفه من قبل الجهات الأمنية، وعدم الإبلاغ عن الجرائم المعلوماتية، وتنازع القوانين وعدم تسليم المجرم من قبل دولته في حالة كون الجريمة

حصلت من خارج قطاع الدولة سواءً كان بسبب تعذر كشفه، أو عدم وجود اتفاقية ثنائية بتسليم المجرمين وعدم التمشي بالاتفاقيات الإقليمية أو الدولية. أدى ذلك كله إلى الانتشار الواسع لجرائم نظم المعلومات.

٣-٣-٧ دوافعها

تتعدد أسباب الجرائم بالقدر الذي تتعدد به المصالح البشرية المتضاربة في مجتمع ما، ولما كانت هذه المصالح بالكثرة التي لا يمكن إخضاعها لحصر فإن أسباب الجرائم لا يمكن إخضاعها لحصر أيضاً (عبد الحميد، ١٤٢٠هـ: ٦٠). ولكن يوجد عدد من الدوافع الشائعة التي تدفع جهة معينة أو فرداً معيناً للقيام بمثل هذه الجرائم أهمها:

١. سياسية: يهدف إلى تدمير أو التجسس على نظام معلوماتي يتبع دولة معادية سواء جهة حكومية أو شركة تنتمي إلى هذه الدولة، وزادت تلك الجرائم ذات الأهداف السياسية، مع ازدياد انتشار الإنترنت.

٢. اقتصادية: يهدف إلى تدمير أو التجسس على نظام معلوماتي لجهة ما كنوع من المنافسة التجارية، كتوجيه مؤسسة صغير إلى مؤسسة كبيرة تسيطر على السوق.

٣. إخفاء المسؤولية: وهو دافع يقع بسبب رغبة الجاني في إخفاء جريمة أخرى أكبر (عبد الحميد، ١٤٢٠هـ: ٦٨)، كخفاء جريمة احتيال معلوماتي بتدمير النظام بالفيروسات أو استخدام القنبلة المنطقية.

٤. الرغبة في الكسب المادي: دافع ينتج بسبب الفقر والعوز أو بسبب الطمع والحقد أو بسبب الرغبة في الإطاحة بمنافس نتيجة لتضارب المصالح التجارية أو بسبب اتخاذ الفرد من الجريمة وسيلة للعيش (عبد الحميد، ١٤٢٠هـ: ٦٨). ونتيجة لتوفير تقنية المعلومات وسيلة إجرامية للثراء السريع والكبير، كتلاعب بالمعالجة الآلية، والاختلاس من الأرصدة الضخمة

٥. إبراز القدرات: ترتكب من قبل أفراد يرغبون في إبراز قدراتهم الفنية لأجل الدفع بالمؤسسات للتعاقد معهم للعمل كاستشاريين، أو إبراز قدراتهم في المحيط الاجتماعي، الذين يعيشون فيه.

٦. تحقيق الذات: يرغب بعض الأشخاص عند حصوله على معرفة معينة أن يحقق لذاته نجاحه بالقيام بها، كالذي يزور عملة ثم يتعامل بها ليحقق النجاح، وليس بدافع مالي، ويقع بعض من جرائم كالاختراق، والتلاعب بالمعالجة الآلية تحت هذا النوع من الدوافع.

٧. التسلية وحب الاستطلاع: القيام بجرائم نظم المعلومات كالاختراقات يعتبرونها أمنية ودليلاً على الذكاء، وفي ظل الانطوائية وعدم التواصل الاجتماعي، وكثرة المنتديات التي توفر المعلومات عن أدوات الاختراق (الشدي، ١٤٢١هـ: ٢١٣)، دفعتهم إلى ارتكاب الجرائم بدافع التسلية.

٨. تحقيق منفعة خاصة: وهو دافع ينشأ بسبب رغبة الجاني في التوصل إلى تحقيق مصلحة خاصة من وراء جريمته (عبد الحميد، ١٤٢٠هـ: ٦٩). ومن أمثلتها ارتكاب جريمة من قبل موظف بداخل مؤسسته لأجل إجبارها باتخاذ إجراء يحقق مصلحه له كتأمين برامج حماية من جهة يرغبها، أو الإضرار بموظف آخر ينافسه، أو قيام شخص بالحصول على معلومات من جهة ما وبيع تلك المعلومات لجهات معينة كالمنظمات الإجرامية، أو مؤسسات منافسة.

٩. الرغبة بالتحدي: العمر النسبي لتقنية حديث نسبياً، كما أن البرامج الجاهزة والمساعدة بالاختراق للأجهزة يساعد الأشخاص الذين يعيشون في أجواء المنافسة والتحدي، أو قد تكون تحدي لتلك المؤسسات التي تضع حواجز أمنية للاختراق (الشدي، ١٤٢١هـ: ٢١٧).

١٠. الانتهازية: يقوم أفراد بانتهاز المؤسسات الكبيرة للحصول على الأموال ثم دفعها إلى الفقراء، حيث يعلل الأشخاص الذين يقومون بتلك الجرائم لأنفسهم بأن أصحاب تلك المؤسسات قاموا باستغلال الفقراء لبناء ثرواتهم (الشدي، ١٤٢١هـ ٢١٩).

١١. التعلم لزيادة المهارة بالحاسب الآلي والإنترنت: يدفع بعض الأشخاص ارتكابه للجرائم بدافع التعلم والتطبيق العملي للمعلومات التي حصل عليها وغالباً يقع تحت هذا النوع من الدوافع جريمة الاختراق.

١٢. الانتقام: يلجأ بعض هؤلاء، إذا ما شعروا بالظلم إلى الانتقام من المؤسسة، وغالباً ما يحصل من أحد الموظفين كالمسؤولين عن إدارة النظام وإدارة الشبكة كرد فعل لإنهاء خدماته من مؤسسته، وغالباً يقع تحت هذا النوع من الدوافع جريمة تدمير المعلومات.

١٣. التنفيس: في حالة الضغوط من جهة ما على فئة اجتماعية معينة، كالاختراقات التي تحدث من بعض الأشخاص في الدول العربية والإسلامية، ضد دول معينة كإسرائيل، والولايات المتحدة الأمريكية في حالة تصاعد مواقف معينة.

١٤. الوصول إلى معلومات شخصية: قيام الجاني إلى الوصول لمعلومات شخصية عن شخص ما لمعرفة أسراره كمعلوماته المالية أو الصحية، أو تقارير كفاءته في عمله.

١٥. خدمة جهات أو أفراد آخرين: دافع يقوم به شخص ما لخدمة جهات أو أفراد بمقابل أو بدون مقابل بسب مهارته الفنية التي يحتاجون منه في ارتكاب جريمة ما، كعمليات الاختراق، أو بعض الجرائم التي تقع في بعض المصارف بتغطية حساب معين برصيد كافي حتى إتمام العملية، أو تمام عمليات مشبوهة كالحولات للمنظمات الإجرامية أو الإرهابية، أو غسيل الأموال، أو إخفاء معلومات شخصية أو بيانات رسمية من الحاسب الآلي كإخفاء المهنة مثلاً، أو إلغاء مبالغ مالية أو فواتير مستحقة الدفع أو مخالفات تجارية أو مرورية وغيرها.

١٦. حب الاستطلاع: طبيعة التقنية إنها تجذب للإطلاع عليها فيرغب الشخص بدافع الاطلاع على كيفية ارتكاب الجريمة، أو الإطلاع على معلومات جهةٍ ما.

١٧. العدوانية: يلجأ بعض الأشخاص للقيام بجرائم نظم المعلومات لإشباع رغباتهم التخريبية يساعدهم بذلك إحساسهم أن لأحد يستطيع ضبطهم.

٤-٣ وسائل التحقيق

عند القيام بالتحقيق Investigation في جريمة ما، يجب على المحقق الالتزام بقوانين، وتشريعات ولوائح مفسرة، وقواعده فنية تحقق الشرعية وسهولة الوصول إلى الجاني (عبد الحميد، ١٤٢٠هـ: ١١). فالمحقق يتبع طريقة ثابتة من الإجراءات المحددة والمحكومة باللوائح المنظمة والقواعد الفنية للتحقيق ليسلكها للوصول إلى الجاني. كما يتبع أساليب متغيرة، كل أسلوب منها يعالج حالة معينة في ظروف معينة. والمحقق يختار أسلوباً واحداً في لحظة واحدة ولكنه قد يلجأ إلى استعمال عدة أساليب متداخلة في لحظات أخرى، حسب اجتهاداته للحالة الماثلة أمامه. فالمحقق يدرس الحالة ويقرر الأسلوب المناسب من خلال دراسته لقضية التحقيق، وبالتالي يحتاج المحقق لوسائل مادية ومعنوية غير محددة ليستخدمها في تنفيذ تلك الطرق الثابتة والمحددة والأساليب المتغيرة وغير المحددة لضبط الجريمة وجمع الأدلة بهدف إثبات وقوع الجريمة ونسبتها إلى الجاني وكسب اعترافه مما يكفل تقديمه إلى العدالة (Geocities, ٢٠٠٢).

وبما أن التحقيق في جرائم نظم المعلومات يحتاج إلى معرفة تامة وأدراك لوسائل تثبت وقوع الجريمة، والوصول إلى الجاني، ونسبتها إليه، تم استعرض وسائل للتحقيق تساعد المحققين للقيام بذلك. وينطلق الباحث من مصادر الدراسة المتعددة. وبناءً على ما استطلعه الباحث مع عينة الدراسة بحكم تخصصهم وخبرتهم كالذين يمارسون التحقيق الإداري بأقسام أعدت للتحقيق في الجرائم الداخلية، واثبات الجرائم التي تقع من الخارج عبر الشبكات، ومنها شبكة الإنترنت، بالإضافة إلى العاملين بالأقسام الأمنية، والتي عهد إليها بالمحافظة على حماية نظم المعلومات، وذلك بالقطاعات الكبيرة (إدارة التقنية البنكية بمؤسسة النقد، وحدة خدمات الإنترنت ومركز الشبكات بمدينة الملك عبد العزيز للعلوم والتقنية، وبعض القطاعات المصرفية، وبعض الشركات الكبيرة).

٣-٤-١ وسائل مادية

يقصد الباحث بها تلك الأدوات الفنية التي غالباً تستخدم في بيئة نظم المعلومات والتي يمكن باستخدامها يتم تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وبما أن غالباً الجرائم التي تقع بواسطة شبكة الإنترنت تكون أصعب في الإثبات وتحتاج إلى تدخل الجهات الأمنية أكثر من جرائم النظم الأخرى التي تعلن عنها المؤسسات، والذين مجرميها غالباً هم من الذين لا يعملون بتلك المؤسسات ولا يخضعون للوائح الداخلية التي يمكن أن تطبقها عليهم. ومن هنا جاء التركيز على الجرائم التي ترتكب عن طريق شبكة الإنترنت وبالرغم من أن الشبكات الأخرى لها نفس الخصائص.

١. عناوين (IP و MAC والبريد الإلكتروني، وبرامج المحادثة)

عنوان الإنترنت (IP) Internet Protocol Address هو المسؤول عن تراسل حزم البيانات عبر إنترنت وتوجيهها إلى أهدافها، ويشبه إلى حد بعيد العنوان على مغلف رسائل البريد التقليدي بعد وضعها بصندوق البريد، وهو يتيح للموجهات والشبكات المعنية بنقل الرسالة (إنترنت العالم العربي، ١٤٢٣هـ). يوجد عنوان (IP) بكل جهاز مرتبط بالإنترنت، ويتكوّن من أربعة أجزاء، والجزء الواحد له ثلاث خانات فيكون المجموع اثنا عشر خانة كحد أقصى ٢٥٥,٢٥٥,٢٥٥,٢٥٥ حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه (Arabiat, ٢٠٠٢).

وفي حالة وجود أي مشكلة أو أعمال تخريبية فإن أول ما يجب أن يقوم به المحققون هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشركة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضاً إذا توفرت لديها أجهزة وبرامج خاصة لذلك أخرى، توجد أكثر من طريقة لمعرفة

عنوان (IP) الخاص بجهاز الحاسب الآلي في حال الوصول المباشر، منها في حالة العمل على نظام تشغيل Windows بكتابة Winipcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP)، مع ملاحظة أنه قد يتغير كلما تم الاتصال بالإنترنت مرة أخرى (Arabiat, ٢٠٠٢). وفي حالة استخدام أحد برامج المحادثة كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى لو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة. كما يمكن الاستعانة بعنوان MAC الذي يحدد أر قام كروت الشبكة MAC للتّعرف على عنوان (IP) بشكل صحيح والذي بدورة يحدد شخصية المتصل (Nor٢٠٠٠, ٢٠٠٢).

٢. البروكسي Proxy

يعمل البروكسي Proxy كوسيط بين الشبكة ومستخدمها، بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات، قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة Cache Memory، يتلقى مزود البروكسي عبر الإنترنت طلباً من المستخدم بحيث يبحث عن الصفحة المطلوبة ضمن ذاكرة كاشي Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فإذا كانت كذلك بالفعل أعادها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية. أما إذا لم يجد مزود البروكسي الصفحة المطلوبة ضمن ذاكرة Cache فإنه يعمل كمزود زبون ويرسل الطلب إلى الشبكة العالمية بحيث يستخدم أحد عناوين (IP)، وأهم مزايا مزود البروكسي أن Cache المتوفر لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة (عبد المطلب، ١٤٢٣هـ: ٢١٩).

٣. برامج التتبع

تقوم هذه البرامج بالتعرف على محاولات الاختراق ومن قام بها وإشعار الجهة المتضررة بعملية الاختراق (الشدي، ١٤٢١هـ: ٣٤)، ومن الأمثلة على تلك البرامج، برنامج Hack Tracer v ١,٢ وهو مصمم للعمل في الأجهزة المكتبية Web وساكناً في خلفية سطح المكتب، وعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ في عملية مطاردة تستهدف اقتفاء اثر مرتكب عملية الاختراق حتى يصل إلى الجهاز الذي حدثت العملية من خلاله، وقد تمت إجراء تجربة عملية على البرنامج محلياً، وتم التأكد من أنه برنامج فعال، وذكر صاحب التجربة، أنه خلال اختبار البرنامج تعرض جهازه، لأكثر من (١٧) محاولة اختراق في فترة قصيرة، وبعد اقتفاء الأثر قاد البرنامج صاحب التجربة إلى أفراد من مدن مختلفة (Arabiat, ٢٠٠٢).

ويتكون البرنامج من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الاختراق التي تحدث ضد جهازه، وتحمل إسم الحدث Event وتاريخ حدوثه، وعنوان (IP) الذي تمت من خلاله، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى. وفور حدوث أي محاولة للاختراق تظهر أمام المستخدم شاشة أخرى صغيرة مصحوبة بتحذير صوتي ويظهر على الشاشة عنوان (IP) الخاص به ويمكن للمستخدم الاختيار ما بين أربعة أوامر موجودة في هذه الشاشة الفرعية منه Report It. والأمر الثاني هوTrace It ، وبمجرد الضغط على هذا الأمر تظهر شاشة أخرى، وعليها إسم الدولة التي تمت منها محاولة الاختراق وعلى المستخدم أن يضغط على أمر NEXT حتى يقوم البرنامج باستكمال عملية اقتفاء الأثر. وبعدها تظهر شاشة ثالثة عليها خريطة العالم وخط طويل ممتد من المدينة التي تمت منها محاولة الاختراق إلى المدينة التي يقيم فيها المستخدم ويوجد اسفل الخريطة مجموعة من الأوامر هيMap وبالضغط عليها تظهر خريطة عليه خط سير محاولة الاختراق (Arabiat, ٢٠٠٢).

والأمر الثاني هو Trace وبالضغط عليه يظهر إسم الشركة المستضيفة وعنوان (IP) ورقم المنفذ Port أو البوابة الخاصة بها. وهناك أمر Network وبالضغط عليه تظهر البيانات الكاملة للشبكة التي تتبعها الشركة المستضيفة للمخترق بما فيها أرقام التليفونات والفاكسات الخاصة بها وآخر تحديث قامت به في جهاز الخدمة الخاص بها وهناك أمرRegistrant ويقدم معلومات الشركة المستضيفة، ثم أمر اقتفاء الأثر وتحديث المعلومات ويظهر علي شكل دائرة عليها خطان متقاطعان، ويمكن الحصول علي هذا البرنامج من موقع www. zdnet.com (Arabiat, ٢٠٠٢). كما يمكن تحديد جهة مرسل الرسائل عن طريق البريد الإلكتروني باستخدام برامج تتبع مصدر الرسائل.

٤. أدوات الضبط

تحتاج جهات جمع الاستدلالات إلى ضبط الجريمة، وإثبات وقوعها، والمحافظة على الأدلة، حتى نسبتها إلى الجاني، لتقديمها إلى هيئة التحقيق والادعاء العام، لكسب اعترافه والذين بدورهم يقدمون تلك الأدلة محفوظة إلى القضاء للمحاكمة. ولذا يوجد أدوات تقوم بضبط الجريمة كغالبية برامج الحماية، وأدوات المراجعة Auditing، وأدوات مراقبة المستخدمين للشبكة، وأدوات التنصت على الشبكة (الداود، أ، ٢٠٠٠م: ٢٤٤)، والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي والتسجيل (الداود، ب، ٢٠٠٠م:١٨٩). وأدوات الضبط الأخرى مثل IDS, MNM٤ Windows, Content Management. كما يمكن استخدام أغلب الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين للمواقع كبرمجيات Java Applets أو Java X، أوCookies والبرامج الأخرى.

٥. الأدوات المساعدة بالتحقيق

يتطلب على المحقق اختيار ما يناسبه من الأدوات التي تساعده في التحقيق، بما قد يواجهه من أن الجاني قد قام بتشفير البرامج، أو غير كلمات المرور، أو أخفى تلك المعلومات أو غير بها،

أو اتلف أدوات الحفظ الخارجية، أو دمر المعلومات بأدوات الجريمة مثل الفيروسات وغيرها ولذا يحتاج إلى أدوات مساعدة. كأدوات استرجاع المعلومات من الأقراص التالفة مثل View Disk، وبرامج كسر كلمة المرور، وبرامج الضغط وفك الضغط Pkzip، برامج البحث عن الملفات العادية والمخفية مثل Xtreepro Gold، برامج تشغيل الحاسب مثل Bootable Diskette، وبرامج نسخ البيانات مثلLap Link (الداود، ب، ٢٠٠٠م: ٢١١). كما يتطلب استخدام برامج منع الكتابة على القرص الصلب بعد ارتكاب الجريمة وذلك لحماية مسرح الجريمة (الطويل، ١٤٢٣هـ: ١٨). وقد يلجأ الجاني إلى حذف الملفات من الحاسب الآلي نهائياً وبالتالي يمكن استرجاعها، ومن الأدوات المهمة لاستعادة تلك الملفات المحذوفة هناك برامج مثل برنامج Windows For Rescue File، وبرنامج Research Regnerud (المجلة الإلكترونية، ١٤٢٣هـ).

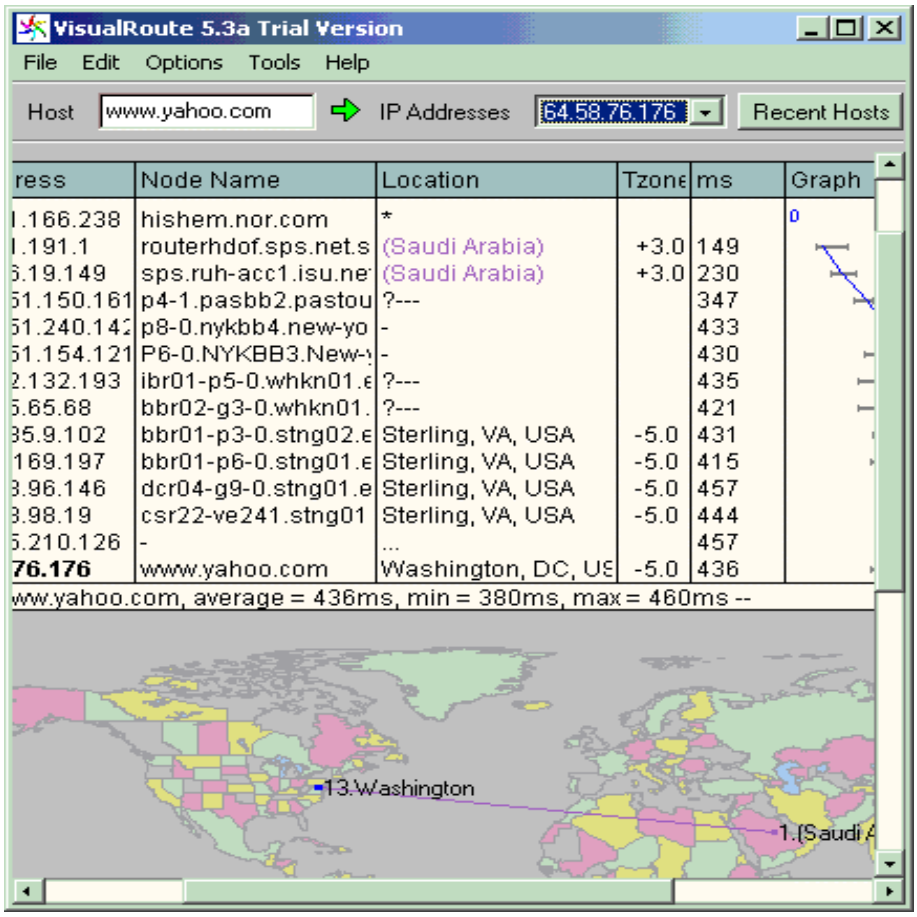
٦. أدوات فحص ومراقبة الشبكات

يمكن أن نستخدم عدد من الأدوات في فحص البروتوكول TCP/IP وذلك لمعرفة المشاكل المتعلقة بالشبكات والعمليات التي تعرضت لها (إنترنت العالم العربي، ١٤٢٣هـ) ومن تلك الأدوات التي يمكن استخدامها على النحو التالي (Nor٢٠٠٠, ٢٠٠٢):

أ. **أداة ARP**: وظيفتها تحديد مكان الحاسب الفيزيائي على الشبكة وهو يحتفظ بجميع أر قام كروت الشبكة MAC، وله عدد من المداخل المستخدمة معه التي تحدد وتعرض كل جدول ARP للتّعرف على عناوين (IP) هل أسندت بشكل صحيح أم لا، ووظيفته الأخرى معرفة رقم كرت الشبكة عند تعين عنوان(IP) خاص لشخص ما.

ب. **برنامج Visual Route ٥،٣a**: هو برنامج يلتقط أي عملية فحص عملت ضد الشبكة فيقوم بإعطاء أجوبة تبين العلميات التي حدث فيه المسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان (IP) أو إسم الجهة برسم البرنامج خط يوضح مسار الهجوم بين مصدره والجهة التي استهدفها ذلك الهجوم، ويوضح الشكل رقم (٥) صورة للبرنامج يبين مسار الهجوم ورسم خطه.

شكل رقم (٥) يوضح صورة لبرنامج Visual Route ٥,٣A والذي يحدد مسار مصدر الهجوم ورسم خطه



المصدر: (Nor٢٠٠٠, ٢٠٠٢)

ج. **أداة TRACER:** ترسم مسار بين جهازين، تظهر فيها كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها و الوقت والقفزات، وهي تسمح برؤية المسار الذي اتخذه (IP) من مضيف إلى آخر، وتستخدم هذه الأداة الخيار ((TTL) Time to Live التي تكون ضمن (IP) لكي تستقبل من كل موجه رسالة (TIME_EXCEEDED)، وبذلك يكون هو العدد الحقيقي للوثبات، ويتم بذلك تحديد بشكل دقيق المسار الذي تسلكه الرزمة، مثال؛ بين متصل من المملكة وبين موقعyahoo.com ويوضح الشكل رقم (٦) صورة لقراءة الأداة ويظهر فيها عنوان (IP) وهو لشركة (أول نت) الشركة المسجل فيها وأخر عنوان (IP) لموقع YAHOO.COM وبين

الاثنين مجموعه من الأرقام التي مر فيها هذا الإرسال، وهذه الأداة تستخدم في الأساس للمسح المبدئي للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف، ولكن يمكن معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي حصلت بها.

شكل رقم (٦) يوضح صورة نتيجة فحص الأداة TRACER للمشكلات التي تقع على الشبكات والمسار.

```
D:\>TRACERT WWW.YAHOO.COM

Tracing route to www.yahoo.akadns.net [216.32.74.50]
over a maximum of 30 hops:

  1   161 ms   150 ms   180 ms  nas3.riyadh.awalnet.net.sa [212.93.193.73]
  2   160 ms   160 ms   160 ms  anr.riyadh.awalnet.net.sa [212.93.193.65]
  3   380 ms   401 ms   350 ms  awalnet.ruh-acc1.isu.net.sa [212.26.63.1]
  4   500 ms   501 ms   511 ms  500.POS3-1.GW10.NYC1.ALTER.NET [157.130.7.189]
  5   491 ms   540 ms   471 ms  571.ATM1-0.XR1.NYC1.ALTER.NET [152.63.26.138]
  6   491 ms   471 ms   490 ms  195.ATM6-0.GW8.NYC1.ALTER.NET [152.63.19.253]
  7   480 ms   481 ms   471 ms  exodus-nyc1-oc12-gw.customer.alter.net [157.130.95.6
6]
  8   561 ms   490 ms   511 ms  bbr02-g3-0.whkn01.exodus.net [216.35.65.68]
  9   460 ms   421 ms   471 ms  bbr02-p1-0.jrcy01.exodus.net [209.1.169.186]
 10   501 ms   500 ms   481 ms  bbr01-p5-0.stng01.exodus.net [209.185.9.98]
 11   561 ms   491 ms   480 ms  dcr03-g10-0.stng01.exodus.net [216.33.96.161]
 12   491 ms   500 ms   491 ms  csr22-ve240.stng01.exodus.net [216.33.98.3]
 13   501 ms   481 ms     *     216.35.210.126
 14   510 ms   381 ms   471 ms  www1.dcx.yahoo.com [216.32.74.50]
```

المصدر: (Nor٢٠٠٠, ٢٠٠٢)

د. **أداة NETSTAT**: هي أداة لفحص حالة الاتصال الحالي للبروتوكول TCP/IP ولها عدد من المهام ومن أهما؛ عرض جميع الاتصالات الحالية ومنافذ التنصت، وعرض المنافذ و العناوين بصورة رقمية، وعرض كامل جدول التوجيه.

٣-٤-٢ وسائل إجرائية

يقصد الباحث بها تلك الإجراءات والتي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والأساليب المتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها.

١. اقتفاء الأثر

أن التركيز على اقتفاء الأثر في جرائم نظم المعلومات أكثر من التركيز على الشهود كما في الجريمة التقليدية، ولعله من المثير للاهتمام أن ما نسبته (٥٠,٠٪) من الجرائم في الولايات

المتحدة تتطلب فحصاً لجهاز الحاسب الخاص بالضحية أو المجرم بحثاً عن دليل للإدانة سواء كان بريداً إلكترونياً أو سجل لغرف المحادثة أو غيرها من الأدلة الأخرى، أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين التي تحمل نصائح، ومن أولها نصيحة هي قم بمسح آثارك cover your tracks فلو لم يقم المخترق بمسح آثاره فإنه سيتم القبض عليه حتى لو قام بالاختراق بشكل سليم. ويمكن تقصي الأثر بطرق عديدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع الأثر للجهاز الذي تم استخدامه للقيام بعملية الاختراق وفي أحد المواقع المتخصصة في أمن المعلومات في الإنترنت تتطرق إلى قصص تعرض المواقع لعمليات اختراق وكيف تم تتبع أثر المخترق والتحكم بجهازه (الفنتوخ، ١٤٢٣هـ: ١٨).

٢. الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته

على المحقق الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما يجب على المحقق الاطلاع على عمليات النظام المعلوماتي، كقاعدة البيانات وإدارتها وخطة تأمينها، ومعرفة موارد النظام، والمستفيدين، والملفات، والإجراءات، وتصنيف الموارد العامة، ومدي مزامنة الأجهزة، ومدى تخصيص للمستفيد وقت معين في اليوم يسمح باستخدام كلمات المرور، ومدى توزيع الصلاحيات على المستفيدين، وإجراءات أمن العاملين، وأسلوب النسخ الاحتياطي. والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد، والبرامج التي تعالج البيانات، وإجراءات نسخ البيانات واستعادتها، والوسائط التي تحتوى على البيانات مثل الأقراص الممغنطة، وتسجيل الوقائع (Logging)، وحالات فشل الدخول إلى نظام، ويحب على المحقق معرفة نوعية برامج الحماية وأسلوب عملها والاستفادة من التقارير Reporting التي تنتجها نظم أمن البيانات، وتقارير Reporting الجدران النارية.

٣. الاستعانة بالذكاء الصناعي

اثبت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليل القرائن، واستنتاج الحقائق، كما يمكن الاستعانة بالذكاء الاصطناعي على حصر الحقائق والاحتمالات والأسباب والفرضيات، ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي وفق برامج صممت خصيصاً لهذا الغرض، تعتمد على نظرية الاحتمالات بعطاء كافة الاحتمالات ثم أكثر الاحتمالات وصولاً ثم الاحتمال الأقوى مع إعطاء الأسباب (البشري، ١٤٢١هـ: ١٨٦).

٤. التوقيف فترة التحقيق

يوصف بأنه وسيلة مهمة من وسائل التحقيق، يعرف التوقيف فترة التحقيق (الحبس الاحتياطي) رجال القانون على أنه " سلب حرية المتهم مدة من الزمن تحددها مقتضيات التحقيق ومصلحته وفق ضوابط قررها القانون " ويعدونه رجال الأمن إجراء من إجراءات التحقيق الجنائي يصدر عمن منحة المشرع هذا الحق ويتضمن أمراً لمدير السجن بقبول المتهم وحبسه به ويبقى محبوساً مدة قد تطول أو تقصر حسب ظروف كل دعوى حتى ينتهي أما بالإفراج عن المتهم أثناء التحقيق الابتدائي أو أثناء المحاكمة و أما بصدور حكم في الدعوى ببراءة المتهم أو بالعقوبة وبدء تنفيذها عليه حيث يحقق بعض عدد من الأغراض كبقاء المتهم في متناول سلطة التحقيق للمحافظة على أدلة الجريمة عن محاولة المتهم إخفائها أو طمسها، إذا أطلق صراحة، ومنع التواطؤ بالحيلولة بين اتصال المتهم بباقي شركائه في ارتكاب الجريمة، وبغل يده عن تجهيز شهود نفى مزيفين، أو من تهديد شهود الإثبات (عرب، ١٤٢٣هـ: ٧١).

٥. إظهار الحقائق

تدرك الجهات الأمنية قلة البلاغات التي تصل إليها من الجهات المتضررة عن جرائم نظم المعلومات (الشدي، ١٤٢١هـ: ٢١٥). كما تتحرك عند تلقي الجهة الأمنية معلومات تشير إلى

وقوع جريمة، أو ضبط أفراد متلبسين، ، أو توفر معلومات من خلال النشر على الشبكة الإنترنت تشير إلى انتشار فيروسات، أو وقوع عمليات اختراق، أو قرصنة (البشري، ١٤٢١هـ: ١٧٩). عند وصول للجهة الأمنية بلاغاً عن جريمة ما يقوم المحقق بالإجراءات التي تتبع تلقي البلاغ من التأكد من صحة البلاغ، والتحفظ على مكان الجريمة وتؤمينه، وتحديد أطراف الجريمة وكل من له صلة بها، وحصر الشهود ومنع مغادرتهم، وحصر الأدلة ورفع الآثار، ويلزم على المحقق إظهار مجموعة من الحقائق في مرحلة جمع الاستدلالات وإثباتها في محضره نظراً لأهميتها في تحديد الجريمة ورسم خطوات البحث في المجهول (عبد الحميد، ١٤٢٠هـ: ٦١). وهي على النحو التالي:

أ. التثبت من توافر أركان الجريمة

يحدد وقوع جريمة ما توفر ركنيين أساسيين وهما الركن المادي ويقصد به الواقعة أو الضرر المادي للجريمة ويتمثل في نشاط الفاعل والنتيجة التي يحققها وعلاقة السبب بينهما والركن الآخر هو الركن المعنوي ويقصد به الإرادة التي اقترن بها الفعل المرتكب ويأخذ صورة القصد الجنائي في الجريمة المتعمدة والصورة الخطاء غير مقصودة (بحر، ١٤٢٠هـ: ٣٨). أن قانون العقوبات حدد لكل جريمة أركاناً معينة يجب توافرها حتى يتم الجزم بوقوعها، ومن البديهي أن أول حقيقة يجب أن يستظهرها محقق جمع الاستدلالات هي التثبت من وجود هذه الأركان ثم الجزم بوجود أو عدم وجود الجريمة، ففي جريمة السرقة مثلاً يجب على الباحث أن يتأكد من أن هناك مالاً منقولاً استولى عليه من شخص غير مالكه بقصد تملكه وهي أركان جريمة السرقة التي أوضحها قانون العقوبات(عبد الحميد، ١٤٢٠هـ: ٦٤)، وهكذا بالنسبة لجرائم نظم المعلومات.

ب. تحديد مكان الجريمة ووصفه

يتوقف التوصل إلى الجاني قدر كبير من نجاح عملية البحث في مكان الجريمة الذي سيوجد فيه الآثار والأدلة الجنائية المتصلة بها، ونتيجة لذلك يعمد كثير من الجناة إدراكاً منهم لهذه الحقائق

إلى نقل هدف الجريمة من مكان إتمام الجريمة وإلقائه في مكان آخر لتضليل المحقق وتعقيد عمليه البحث (عبد الحميد، ١٤٢٠هـ: ٦٥).

ج. تحديد وقت وقوع الجريمة

يتضمن تحديد وقت الجريمة تحديد تاريخ وساعة وقوعها، ويتم ذلك التحديد من أقوال المجني عليه أو المبلغ أو الشهود وقد يتم عن طريق الخبراء والمتخصصين، وهو عنصر هام لتحديد مسئولية المتهم في ارتكاب الجرائم وذلك عند مناقشته عن خط سيره والأماكن والأشخاص الذين كان بصحبتهم في الفترة المعاصرة لارتكاب الجريمة واكتشاف مدى صدق البلاغ وصحة شهادة الشهود، بالإضافة إلى أن الوقت في بعض الجرائم تعد ظرفاً مشدداً (عبد الحميد، ١٤٢٠هـ: ٦٦). ولذلك يجب على المحقق الاطلاع على التوقيتات التي تظهرها برامج الحماية والتطبيقات.

د. تحديد أسلوب ارتكاب الجريمة

الأسلوب هو الكيفية المتغيرة في طريقة الوصول إلى الهدف التي اتبعها الجاني في ارتكاب جريمته. ويدخل تحديد الأسلوب في الحقائق الجوهرية التي يجب أن يستوضحها المحقق نظراً لأهميته القصوى في تحديد خطة البحث عن الجاني في الجرائم، فكما أن لكل مجرم أسلوبه الإجرامي الذي لا يغيره إلا نادراً، فمن الأسلوب يستطيع المحقق حصر قطاعاً محدداً من المجرمين يركز البحث عن الجاني بينهم، ويكون التسجيل الجنائي مفيداً في تحديد أسلوب ارتكاب الجريمة ومعرفة مجرمين اعتادوا ارتكاب الجرائم المشابهة للجريمة المرتكبة (عبد الحميد، ١٤٢٠هـ: ٦٢). ومثالها زراعة برامج اختراق وتجسس أو الحصول على المعلومات فهذا الأسلوب يقوم به من أراد الحصول على معلومات ولا يستطيع الاقتراب من مصدرها ويكون التركيز على من يقوم بصيانة لتلك الأجهزة، وينحصر البحث على موظفي الصيانة والتشغيل بالمؤسسة، أوأسلوب تغيير الإعدادات فغالباً يقوم به المبرمجين الذين يعملون بالمؤسسة.

هـ. تحديد أداة ارتكاب الجريمة

تحديد الأدوات المستخدمة أمر جوهري لتحديد شخص الجاني، وتحديد الأشياء التي يقع على الباحث عبء التفتيش بحثاً عنها وضبطها (عبد الحميد، ١٤٢٠هـ: ٦٣). ومن أمثلة الأدوات Net Bus، Sub Seven، Hack a Tack، Win Crash، وبرامج التنصت على الشبكات، وأقراص بدء التشغيل، وغيرها.

و. إيضاح الظروف المحيطة بالجريمة

يستوجب على المحقق إيضاح الظروف التي تحيط بالجريمة، ومعرفتها. وتعد خطوة المحقق الأولى في تحديد ومعرفة سبب ودوافع الجريمة، وبعض هذه الظروف يكون سابقاً على وقوع الجريمة. ومثالها سوء سمعته المتهم وسلوكه والشكاوى والمشكلات السابقة التي حدثت بالمؤسسة وبعض الظروف المعاصرة ارتكاب الجريمة ومن أمثلته مكان وجود المتهم حال الجريمة، وتحديد درجة الإضاءة، وساعة ارتكاب الجريمة، وبعض هذه الظروف لاحق على ارتكاب الجريمة ومن أمثلته تصرفات وسلوك من تحوم حولهم الشبهات بعد ارتكاب الجريمة، (عبد الحميد، ١٤٢٠هـ: ٦٨).

ز. تحديد دوافع الجريمة

من الأمور المهمة التي يسعى المحقق لكشفها معرفته دوافع الجريمة، ويعني سبب الجريمة الوقائع المادية التي حدثت فأثرت في نفسية الجاني مما أدى إلى بروز الدافع على ارتكابه للجريمة وهو أمر نفسي داخلي يرتبط أساساً بمجموعة من الغرائز الإنسانية وهو يتبلور عادة في بروز حاجة ما تدفع الشخص إلى توجيه سلوكه لإشباعها، فتحديد السبب في بعض الجرائم يشكل في حد ذاته دليلاً على ارتكاب المتهم للجريمة، ويكفل تحديد السبب حصر دائرة البحث في عدد محدد من الأشخاص، وبالعكس فإن عدم تحديد أسباب الجريمة يربك المحقق لتعدد الطرق التي يجب عليه أن يسلكها في بحثه لكشف الجريمة ويطيل من فترة البحث مما قد يوقعه في دائرة اليأس من كشف

الجريمة، ويؤخذ عدم وضوح سبب ودوافع الجريمة كدليل نفي قد يشير إلى براءة من تحوم حوله الشبهات مما قد يؤدي إلى استبعاده من قائمة الاتهام أو الحكم ببراءة إذا كان الاتهام قد وجه إليه (عبد الحميد، ١٤٢٠هـ: ٦٩).

وفي جرائم نظم المعلومات غالباً يصبح من الصعب جداً معرفة سبب الحادث وذلك لأن دوافع الجناة غير واضحة، أو قد تحدث الجريمة بالخطاء، أو أن الجاني لا يحدد هدفاً للجريمة وهذا راجع لأسلوب ارتكاب الجريمة حيث كمجرم نظم المعلومات الذي يبحث في المنافذ المفتوحة فقط في أي جهاز حاسب آلي ليصبح كتلك القاتل المأجور الذي يصعب اكتشاف جريمته. وهناك عدة عوامل تساعد المحقق في تحديد سبب الجريمة ومن أهم هذه العوامل ما يلي (عبد الحميد، ١٤٢٠هـ: ٧١):

- نوع الجريمة: غالباً يحدد سبب ارتكابها، فنجد أن جريمة سرقة الأقراص يتحدد سببها بالحصول على المعلومات، وسبب ارتكاب جرائم تدمير المعلومات يكون الانتقام هو الدافع.
- هدف الجريمة: تشير في بعض الأحيان إلى سبب الجريمة، كالمبرمج الذي يضع القنبلة الموقوتة في النظام لدرء مسئوليته عن اكتشاف جريمة يريد إخفاءه.
- المعاينة: تشكل عاملاً هاماً لكشف سبب الجريمة فمعاينة مسرح الجريمة يسفر عن اكتشاف الجريمة، فمثلاً وجود بعض البرامج المزروعة كالفيروسات تشير في حد ذاتها إلى أن الدوافع من وراء هذه الجريمة هو الانتقام، أو العدوانية.
- تحديد مكان الجريمة ونوع الخدمة المقدمة: يمكن أن يدل على تحديد مكان الجريمة ونوع الخدمة المقدمة سبب في كشفها بغض النظر عن مكان الجاني كوقوع الجريمة في مصرف مالي يقدم خدماته عبر الشبكات.

- أقوال المتضررين والشهود: وهؤلاء يشكلون عاملاً حاسماً في تحديد سبب الجريمة إذا ما أحسن الباحث مناقشتهم والإحاطة بظروف كل منهم.

- أهل الخبرة: أحد أعوان الباحث الذين يرشدونه كثيراً عن الأسباب المحتملة لوقوع الحادث، ومثال ذلك تقصي أثار الجاني، وأساليبه، والأدوات التي استخدمها قد يحدد سبب الجريمة.

٦. إتباع القواعد الفنية لكشف الجريمة

أن عمل المحقق يبدأ منذ الوقت الذي يصله فيه خبر وقوع جريمة، ويقوم بالإجراءات التي يتخذها عقب ذلك من معاينة وتفتيش وانتداب للخبراء وسماع للشهود واستجواب لأطراف الجريمة، وجمع التحريات، وهو في كل هذه الإجراءات يستخلص العديد من الأدلة ويحاط علماً بكثير من الوقائع المتصلة بالجريمة والتي تختلف في قوة ثبوتها، وتأتي في أعقاب ذلك مرحلة يجد المحقق فيها نفسه وأمامه مجموعة ضخمة من الأدلة والوقائع التي أمكنه جمعها، ولمحاولة كشف الجريمة على المحقق التقيد بالتالي (عبد الحميد، ١٤٢٠هـ: ٣١٤):

أ. مراعاة الاحتمالات الشائعة في الجرائم

لا يمكن حصر الاحتمالات نتيجة لتعذر واختلاف هذه الاحتمالات حسب ظروف وأسباب كل جريمة، إلا أن هناك مجموعة من الاحتمالات التي يضعها المحقق عادة في كونه عند فحصه لبعض أنواع الجرائم كاحتمال عدم وجود جريمة أصلاً أو احتمال كذب البلاغ أو تصويره على غير حقيقته، كذلك احتمالات الظروف المحيطة بالجريمة كهل وقعت الجريمة فجأة ونتيجة لظروف عارضة أم أنها متصلة بحوادث أخرى وسبقها تهديد من الجاني، وهل الجاني فرد واحد أم عدة أفراد هل كان على صلة بالضحية أم لا، وهل هو أحد الموظفين أو المتواجدين أساساً بالمؤسسة أم هو شخص من الخارج، وتتضمن الاحتمالات الأساليب المختلفة التي يمكن أن يرتكب بها الحادث.

ب. تقدير احتمالات وقوع الجريمة

يقصد باحتمالات وقوع الجريمة الخطوات التي يتصور المحقق أن الجريمة قد سارت فيها منذ مرحلة نشوء أسبابها والتفكير فيها والتحضير لها ثم تنفيذها وهي الأدوار التي تمر بها الجرائم عادة، والمحقق في تصوره لهذه المراحل يعتمد أساساً على الأدلة والوقائع التي تمكن من جمعها خلال مراحل بحثه في الجريمة وذلك بإتباع طرق متعددة عند فحصه لهذه الأدلة، كما أن التصورات التي يمكن أن يستخلصها من هذه الأدلة تختلف حسب نوع الجريمة التي يبحثها، ومن طرق تحديد الاحتمالات تحليل الأدلة التي لا بد وأن تشير إلى مدلول محدد أو عدة مدلولات تتصل بالجريمة التي يجري بحثها، كما أنه يفضي إلى مجموعة من الاستنتاجات التي يمكن تصور حدوثها نتيجة لوجوده، كما يترتب عليه استبعاد عديد من الوقائع التي يتنافى وجودها مع وجوده فضلاً عن مساهمته في إعطاء صورة تقريبية لمكان وقوع الحادث، والمحقق عندما يحلل ما حصل عليه من أدلة ووقائع بالصورة السابقة يبني في نفس الوقت الاحتمالات الممكنة لوقوع الجريمة التي يبحثها.

ج. فحص الاحتمالات

بعد أن يحصر المحقق الاحتمالات التي يمكن أن تقع على أساسها الجريمة وذلك في ضوء مدلولات الأدلة والحقائق التي استنتجها منها وما استبعده من احتمالات نتيجة لها وما استخلصه من تصورات لكيفية ارتكاب الجريمة يبدأ بعد ذلك في فحص كل احتمال من هذه الاحتمالات متبعاً في ذلك القواعد الفنية رسم خطة البحث، والبدء بالاحتمال الأقوى، وعدم التشبث باحتمال واحد، وعدم التعجل للوصول إلى نتيجة إيجابية من فحص الاحتمال.

٣-٥ عوائق استخدام وسائل التحقيق

يتسم التحقيق في جرائم نظم المعلومات بشكل عام بالعديد من المعوقات والتعقيدات التي يمكن أن تعرقل من عملية التحقيق أو تؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسيه المحقق

بفقدان الثقة في نفسه وفي أدائه وعلى المجتمع بفقدان الثقة في جهاز الأمن غير القادر على حمايته من هذه الجرائم وملاحقة مرتكبها، وانعكاسها أيضاً على المجرم نفسه، حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق لا تجاري خبرته وعلمه، الأمر الذي يعطيه ثقة كبيرة في ارتكاب جرائم أكثر فداحة وضرراً على المجتمع المحلي أو المجتمعات الأخرى عبر نظم المعلومات (بحر، ١٤٢٠هـ: ٥١). يواجه استخدام وسائل التحقيق عند الأجهزة الأمنية معوقات متنوعة يمكن استعراضها على النحو التالي:

١. عوائق متعلقة بالتشريع

بانعدام القوانين والعقوبات ضد كل من يرتكب جرائم نظم المعلومات فإن ظاهرة هذه الجرائم ستتفاقم وتصل إلى مرحلة تصبح فيها عملية العلاج لهذه الظاهرة أصعب مما يتوقع خصوصاً وأن جميع المعاملات والإجراءات التجارية والحكومية سيتم التعامل معها عن طريق نظم المعلومات، كما أن معظم المحاكم لا تعتمد الأدلة والقرائن التي توفرها الجهات الأمنية عند المداهمة والتحقيق مع مجرمي نظم المعلومات، وذلك ناتج عن غياب القوانين والعقوبات التي يجب وضعها بشكل مشترك بين الجهات المسؤولة عن أمن المعلومات والأمن العام وهيئة التحقيق والادعاء العام والجهات القضائية والتشريعية (الحمادي، ١٤٢٣هـ: ٢٩). أن التشريعات والقوانين المحلية والدولية تمثل الإطار العام الذي يمكن من خلاله تحديد ما إذا كان الفعل المرتكب يمثل جريمة من عدمه (بحر، ١٤٢٠هـ: ٤٩).

كما أن غياب المعاهدات والاتفاقيات الدولية بين دول العالم لإثبات التهم على مجرمي نظم المعلومات أو القبض عليهم وتسليمهم للجهات الأخرى أو محاكمتهم، وقد يمكن تطبيق الأنظمة الحالية التي تتعامل مع جرائم نظم المعلومات باعتبارها جرائم سرقة ونصب واحتيال وتخريب وغيرها، شأنها في ذلك شأن الجرائم في الحياة العامة التي يطبق فيها تلك الأنظمة مما سيكون أثره إيجابي في الحد من جرائم النظم، أن عدم وجود قوانين وعقوبات ضد كل يرتكب جرائم نظم

المعلومات فإن ظاهرة هذه الجرائم ستتفاقم وتصل إلى مرحلة تصبح فيها عملية العلاج لهذه الظاهرة أصعب مما يتوقع خصوصاً وأن جميع المعاملات والإجراءات التجارية والحكومية سيتم التعامل معها عن طريق نظم المعلومات، فوضع القوانين والعقوبات من أهم الإجراءات المهمة التي يجب البدء في وضعها في أقرب وقت ممكن (الحمادي، ١٤٢٣هـ: ١٥). ومن هنا يمكن القول أن عدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في هذا البلد يعد عائقاً للتحقيق.

٢. عوائق متعلقة بالجريمة

كخفاء الجريمة، وغياب الدليل المرئي الممكن بالقراءة فهمه، وافتقاد أكثر الآثار التقليدية وإعاقة الوصول إلى الدليل بوسائل الحماية الفنية، وسهولة محو الدليل أو تدميرها في زمن قصير جداً، والضخامة البالغة لكم المعلومات والبيانات المتعين فحصها، وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة (الجاني) والضحية (المجني عليها) (بحر، ١٤٢٠هـ: ٤٦). كما أن هناك معوقات أخرى للتحقيق تتعلق بالجريمة مثل معوق عدم المعرفة بمكونات عناصر جريمة نظم المعلومات من قبل الأطراف المعنية، ومعوق إمكانية ارتكاب جرائم نظم المعلومات عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط.

٣. عوائق متعلقة بالجهات المتضررة

أن عدم إدراك خطورة جرائم نظم المعلومات من قبل المسؤولين بالمؤسسات تعد أحد معوقات التحقيق. كما يعد إغفال الجانب التوعوي لإرشاد المستخدمين إلى خطورتها معوق أخر، وبالنظر إلى بعض المؤسسات نجد أنها أسست نظم معلوماتها على تطبيقات خاصة من التقنية على أساس أنها تقدم لعملائها خدمات أسرع بدون عوائق ويكون ذلك على حساب الأمن (الحمادي، ١٤٢٣هـ: ١٤). كما تعد التقنية المستخدمة في نظم المعلومات مجال استثمار ولذا تتسابق الشركات بتبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم تركيز على الجانب الأمني. على سبيل المثال مستخدمي شبكة

الإنترنت عبر مزودي الخدمة أو بطاقات الإنترنت المدفوعة ليسوا مطالبين بتحديد هويتهم (عملية ربط رقم المستخدم مع هويته) عند الاشتراك في خدمة الإنترنت أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة (الحمادي، ١٤٢٣هـ: ١٤). كما أن الإحجام عن الإبلاغ عن الأشخاص الميسورين أو صغار السن، خوفاً من المجتمع المحيط بهم وخشية الفضيحة معوق من معوقات التحقيق (بحر، ١٤٢: ٣٩).

كما يكون الإحجام عن الإبلاغ عن جرائم نظم المعلومات بسب عدم رغبة الجهات المتضررة الظهور بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما يوحي بإهمالها أو قلة خبرتها، أو عدم وعيها الأمني (الشدي، ١٤٢١هـ: ٢١٠)، ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها (الحمادي، ١٤٢٣هـ: ٢٣). كما يوجد أسباب أخرى تحجم الإبلاغ عن جرائم نظم المعلومات من قبل الجهات المتضررة، كالتالي (الشدي، ١٤٢١هـ: ٢١٠):

أ. الحفاظ على سمعة المؤسسات ومصداقيتها فمثلاً تعرض المصارف المالية إلى سرقة لأرقام بطاقاتها الائتمانية أو اختراق لنظم معلوماتها، فأنها لا ترغب لأحد بالاطلاع عليها، فقد يسبب إساءة لسمعتها، وفقدان لمصداقيتها أمام العملاء، ويزيد من سمعة منافسيها، وبالتالي لا تقوم بالإبلاغ عن الحوادث حفاظاً على سمعتها.

ب. بعض ما يصنف على أنه جرائم معلوماتية يكون محدود الأثر، مما قد يدفع بعدم الإبلاغ عنها، فقد يقوم مخترق ما للنظام بإظهار رسالة تفيد بقيامه بهذه العملية، أو يقوم مجرم آخر بإرسال فيروس حاسب آلي إلى جهاز المستفيد ويكون هذا الفيروس محدود الأثر، أو تقوم برامج الحماية من الفيروسات بالقضاء عليه. ولاشك أن توعية المستخدمين بالإفصاح عن مثل هذه الجرائم أمر حتمي لأن الاختراق حتى لو حدث دون آثار في الوقت الحاضر قد يكون مدمراً في المرات الأخرى أو قد لا تعرف حدود آثاره.

ج. الإفصاح عن التعرض لجريمة معلوماتية قد يؤدي إلى حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتي. فقد يحرم الموظف في المنظمة من خدمات معينة على الإنترنت أو قد يحرم من خدمات الإنترنت عموماً حين التعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها.

د. تتبنى جميع الشركات الصانعة للأجهزة والبرمجيات نظاماً يتعلق بضمان سلامة الأجهزة أو البرامج التي تصنعها، وتمتد فترة الضمان لمدد مختلفة حسب نوع المنتج. فإذا كان تأثير الجريمة المعلوماتية يدخل ضمن المواد التي يشملها عقد الضمان فلا يتم الإبلاغ عن هذه الجريمة للاستفادة منه، خاصة إذا كان عقد الضمان يشمل عدم المسؤولية عن الخلل الناتج عن مثل هذه البرامج أو الجرائم المعلوماتية، كما تقوم معظم المؤسسات بالتأمين على الأجهزة والبرامج والبيانات، وتخضع المواد المؤمن عليها لبعض الاشتراطات لانطباق التأمين عليها قد لا يكون من ضمنها التعرض لمثل هذه الجرائم المعلوماتية التي تحدث بسبب الإهمال وخلافه، فلا يقوم الشخص أو المؤسسة بالإبلاغ عن مثل هذه الجرائم.

هـ. الإعلان عن جرائم نظم المعلومات، أو الإعلان عن الاحتياطات الأمنية المشددة، يعطيهم الإحساس بقدرتهم على النجاح، وقد يكون دافعاً لمرتكبيها لإعادة المحاولة مرة أخرى، وكأنه تحدي لكل من عنده نواي إجرامية أن يحاول اختراق النظم.

و. لا يفصح سواءً المستخدمين أو المتخصصين أو مسئولي أمن المعلومات عن مثل هذه الجرائم التي حدثت للنظام والتي قد يكون إخفاق إجراءات أمن النظام سبباً لها فلا يفصحون عنها خوفاً من المساءلة أو فقدان الوظيفة.

ز. قد يكون سبب عدم الإبلاغ عن الجريمة، عدم معرفة الضحية بوجود جريمة أصلاً، وعدم القناعة إنها ممكن أن تحدث في مؤسسته.

والخلاصة يمكن القول أن أهم المعوقات المتعلقة بالجهات المتضررة هي؛ معوق معظم المؤسسات المتضررة من جرائم نظم المعلومات لا تتقدم بشكوى للجهات، ومعوق عدم قناعة العاملين بمجال نظم المعلومات في تدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية، ومعوق عدم وجود مردود مادي ملحوظ لتحديث برامج الحماية والتحقيق، ومعوق مقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية، ومعوق عدم وجود قسم متخصص في جرائم نظم المعلومات، عائق عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق، معوق عدم تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية، ومعوق عدم التنسيق بين المؤسسات المستخدمة لنظم المعلومات والشركات الموفرة لأمن المعلومات، ومعوق عدم التنسيق بين والجهات الأمنية والمؤسسات المستخدمة لنظم المعلومات.

أما الإحجام عن الإبلاغ؛ يشمل معوق الحفاظ على سمعة المؤسسات ومصداقيتها، ومعوق عدم رغبة الجهات المتضررة الظهور بمظهر الضحية ومعوق محدودية الآثار المترتبة على الجريمة، ومعوق الخوف من الحرمان من الخدمات المقدمة الاستفادة من خدمات الضمان، ومعوق الرغبة في عدم إبراز كفاءة المجرمين، ومعوق الخوف من المسؤولية، ومعوق عدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع.

٤. عوائق متعلقة بجهات التحقيق

أ. عدم التدريب

اهتمت أجهزة الأمن في الكثير من دول العالم لمواجهة جرائم النظم والتحقيق فيها (بحر، ١٤٢٠هـ: ٤١)، ففي الولايات المتحدة الأمريكية، تمثل أعلى نسبة من المستخدمين لنظم المعلومات في العالم وتعاني بشكل كبير من الجرائم المرتكبة عبر تلك النظم، مما دعاها إلى إنشاء وحدة متخصصة للمكافحة والتحقيق في جرائم نظم المعلومات من ضمن مكتب التحقيقات الفيدرالي FBI، ويكون تدريب عناصر هذه الوحدة مستمراً ليواكب تطورات جرائم التقنية

(Vacca, ١٩٩٦)، ومن ضمن المعاهد التي يعهد إليها بتدريب تلك المجموعة، هو معهد أمن الحاسب الآلي (Compute Security Institute)، بالإضافة إلى عملة بإعداد التقارير الأمنية حول مخالفات أمن المعلومات (CSI, ٢٠٠٢)، ويتركز تدريب هذه العناصر في إعطائهم دورات تدريبية في استخدام الحاسب الآلي وكيفية عمله واستخدام شبكة الإنترنت وكيفية عملها وخدماتها وأنواع جرائم الحاسب الآلي وجرائم الإنترنت وأساليب ارتكابها وأساليب التحقيق فيها وقانون الإجراءات في مجال جرائم الحاسب الآلي وجرائم شبكة الإنترنت (Ressler, ١٩٩٧).

ب. عدم الاستعانة بالخبراء

تقوم بعض الجهات بتقديم مساعدتها للجهات الأمنية في مجال التحقيق بجرائم نظم المعلومات بتقديم التقارير عن الجرائم التي تتبعها، والمعلومات الإحصائية عن تلك الجرائم، والمساعدة في تحديث للوائح والتشريعات، وعقد المؤتمرات، كتلك الجهات التي تساعد FBI مثل جمعية التحقيق في جرائم الحاسب FACCI The Florida Association Of Computer Crime Investigators (FACCI, ٢٠٠٢). أو منظمة طوارئ الحاسب والمستشارون في أمن المعلومات CERT* (CERT, C, ٢٠٠٢) Advisories Of Security Information. أو معهد أمن الحاسب (CSI) Compute Security Institute.

ج. عدم توفير الكفاءة البشرية المؤهلة للتحقيق

تتركز على جهات مكافحة الجريمة، كمعوقات التحقيق المتعلقة بشخصية المحقق؛ مثل التهيب من استخدام الحاسب الآلي، والتهيب من استخدام شبكة الإنترنت، وكذلك عدم الاهتمام بمتابعة المستجدات في مجال جرائم نظم المعلومات. ومعوقات التحقيق الفنية؛ كالمهارة الفنية المطلوبة للتحقيق في جرائم نظم المعلومات لدى المحقق، ومهارة استخدام الحاسب الآلي والإنترنت، والمهارة الفنية للتحقيق في جرائم الحاسب الآلي والإنترنت، والمعرفة بمصطلحات الحاسب الآلي وشبكة الإنترنت، ومعرفة أساليب ارتكاب جرائم الحاسب الآلي والإنترنت،

والخبرة في مجال التحقيق في جرائم الحاسب الآلي والإنترنت والمعرفة باللغة الإنجليزية (بحر، ١٤٢٠هـ: ٥٤).

ومن هنا يمكن القول أن أهم معوقات التحقيق المتعلقة بجهات المكافحة هي؛ معوق عدم توفير الأجهزة والبرامج المناسبة للتحقيق، ومعوق عدم توفير المتخصصين والخبراء في الحاسب الآلي بالأجهزة الأمنية، ومعوق عدم التدريب في معاهد متخصصة بالتحقيق في جرائم نظم المعلومات، ومعوق عدم التنسيق بين المحققين بالأجهزة الأمنية والعاملين في مجال نظم المعلومات، ومعوق عدم توفير الكفاءة البشرية القادرة ويشمل؛ معوق عدم توفر المهارة العالية لاستخدام الحاسب الآلي والإنترنت، ومعوق عدم المعرفة بمتطلبات أمن المعلومات، ومعوق عدم المقدرة على إتباع السياسة الأمنية للتعامل مع الجرائم، ومعوق عدم المعرفة بأساليب ارتكاب جرائم نظم المعلومات، ومعوق عدم المقدرة على الإثبات الجنائي.

٣-٦ الأدلة المثبتة

٣-٦-١ أنواع الأدلة المثبتة

تتنوع الأدلة، حيث يمكن أن تصنف على النحو التالي:

١. من زاوية قوتها الإثباتية: هناك أدلة مباشرة تثبت الجريمة بصورة مباشرة، وأدله غير مباشرة تنصب على وقائع لا تشير إلى الجريمة مباشرة وإنما يحتاج الأمر إلى إعمال العقل والمنطق لاستخلاص الأدلة منها (عبد الحميد، ١٤٢٠هـ: ١٨٦).

٢. من زاوية النتيجة القضائية المستخلصة منه؛ هناك دليل يدل على وقوع الجريمة، ودليل على تحديد شخص مرتكبها، ودليل يثبت ارتكابها على المتهم (عبد الحميد، ١٤٢٠هـ: ١٨٧).

٣. من ناحية وظيفة الدليل الإثباتية؛ فهناك أدلة تنصب على إثبات توافر أحد ركني الجريمة المادي أو المعنوي، وهناك أدلة تنصب على تحديد شخصية المتهم. فأما التحديد القاطع فيشير إلى تحديد شخصية الجاني دون أدنى شك، كالبصمات، وآثار الأقدام العارية، والشهادة بالرؤية، والاعتراف، وضبط محصلات الجريمة في حوزة المتهم، وآثار المقاومة على جسده أو بأظافر المجني عليه، أو التحديد غير القاطع يشير إلى مجرد احتمال لتحديد شخصية الجاني وهي مجرد قرائن (عبد الحميد، ١٤٢٠هـ: ١٨٧).

٤. من زاوية مضمون الدليل؛ هناك أدلة مادية محسوسة بإحدى الحواس، وهناك أدلة معنوية مثل الشهادة وأدلة قوليه مثل أقوال المتهم (عبد الحميد، ١٤٢٠هـ: ١٨٨)، وأدلة قانونية ويقصد بها الأدلة التي حددها المشرع وعين حالات استخدامه ومدى حجيتها، وأدلة فنية (أبو القاسم، ١٩٩٤م)، بالإضافة إلى تلك الأنواع "هناك نوعاً آخر من الأدلة وهي الأدلة الرقمية (الإلكترونية)" (البشري، ١٤٢٣هـ: ١١٠). وبالرغم أن هناك من يعد تلك الأدلة الإلكترونية مرحلة متقدمة من الأدلة المادية، أو أدلة فنية لأنها تنبعث من رأي الخبير الفني، إلا أن (البشري) يعدها نوعاً متميزاً من وسائل الإثبات. وذلك بسبب كونها نبضات غير محسوسة، وأن حجمها وشكلها تخيلي وأنها سريعة الانتقال. ويمكن استخراج نسخ من الأصل والحصول على نفس الدليل الموجود بالمسرح الجريمة التقليدي بالمسرح الإلكتروني أو بمسرح إلكتروني آخر، وقد يكون بمقدور المحققين استرجاع الدليل بعد حذفه (البشري، ١٤٢٣هـ: ١١٥).

٣-٦-٢ نماذج من الأدلة الإلكترونية المثبتة

يتم التركيز في هذه الدراسة على الأدلة الإلكترونية لاحتياج تلك الأدلة إلى مزيد من التوضيح لأهميتها في الإثبات الجنائي عند التحقيق في جرائم نظم المعلومات من وجهة نظر الباحث، ومن هذه النماذج ما يلي:

١. ما تحتفظ ملفات تسجيل الدخول بالوقائع المدونة بها، كقيام فرد باختراق النظام وتمكن من إضافة رقم خاص به (داود، ب، ٢٠٠م: ٢٥٥).

٢. وجود عمليات دخول للنظام في الأوقات المتأخرة من الليل أو أيام الإجازات مؤشر على أن هناك جريمة حدثت بغياب العاملين (الشدي، ١٤٢١هـ: ١٤٤).

٣. عمليات نسخ ملف كلمات المرور، أو وجود أفراد غير مسجلين أصلاً في نظام الملف، يوحي بأن جريمة قد تمت أو مازالت في طور الإعداد لها عن طريق استخدام الاسم وكلمة المرور للوصول إلى ملفات النظام (الشدي، ١٤٢١هـ: ٩٤).

٤. يفيد سجل صلاحيات المستخدمين عند حدوث أي تغييرات غير نظامية في صلاحيات أي من المستخدمين يعد دليل على جريمة وقعت أو جريمة سوف تقع (داود، ب، ٢٠٠م: ٢٦٦).

٥. قد يكشف مراجعة البرامج العاملة واختبارها أدلة تثبت وقوع جريمة نظم المعلومات، كتغيير الإعدادات، أو وضع حصان طروادة، أو القنابل المنطقية وغيرها من الجرائم ذات الصلة بكتابة تعليمات البرامج (الشدي، ١٤٢١هـ: ١٠٤).

٦. ما تكشفه برامج الحماية عند إرسال فيروسات وأحصنة طروادة وبقية أدوات الاختراق تعد أدلة على وقوع جريمة.

٧. تؤدي عمليات التحديث والتغيير في النظم إلى اكتشاف أدلة تثبت وقوع جرائم نظم المعلومات (الشدي، ١٤٢١هـ: ٢٠٦).

٨. يعطي النظام المعلوماتي عند حصول جريمة أدلة الإلكترونية تظهر بشكل تغيرات على النظام كتغيير مفاجئ يظهر في الأجهزة يعد دليل قوي على وجود عملية اختراق مبطنه (المجلة الإلكترونية، ١٤٢٣هـ).

٩. ظهور تغيير في شاشة إقلاع الجهاز عند بدء التشغيل هو دلالة واضحة على نجاح عملية اختراق. وظهور ملفات جديدة بشكل مفاجئ في أدله القرص الصلب، حيث أن طرق اختراق الأجهزة تجاوزت زرع ملفات التجسس بسجلات وأصبحت تلك الملفات تزرع مباشرة ضمن القرص الصلب أو ضمن سطح المكتب أو على شريحة البايوس مباشرة (المجلة الإلكترونية، ١٤٢٣هـ).

١٠. يعد البطء المفاجئ المصاحب لتحميل المواقع أو التطبيقات الجديدة أو عند تنزيل البرامج من الإنترنت إشارة علي وجود عمليات اختراق (مجلة الأمن الإلكترونية، ١٤٢٣هـ).

١١. ما يحتفظ به الحاسب الآلي من بيانات مخزنه به أو بالأدوات الملحقة به أو المنقولة عبر شبكاته، كالبيانات المنقولة عبر البريد الإلكتروني، وبرامج المحادثة، ووسائل الاتصالات (البشري، ١٤٢٣هـ: ١٠٢).

١٢. "ما يتم استرجاعه من المعلومات التي تم حذفها، أو إخفاءها، أو المعلومات التي تم فك تشفيرها (البشري، ١٤٢٣هـ: ١٠٣).

١٣. البيانات الناتجة عن برنامج Visual Route ٥,٣a (٢٠٠٢ ,Nor٢٠٠٠). وبرامج تتبع الاختراق كبرنامج Hack Tracer v ١,٢ (Arabiat, ٢٠٠٢). وبرامج تتبع جهة مرسل الرسائل عن طريق البريد الإلكتروني.

١٤. ما تكشفه الأدوات (IP) (Arabiat, ٢٠٠٢)، و(MAC) (٢٠٠٢ ,Nor٢٠٠٠). والبرامج التي تشغل البريد الإلكتروني، والبيانات برامج المحادثة) من بيانات توضح شخصية مرتكب جرائم نظم المعلومات سواء بطريقة مباشرة أو غير مباشرة.

١٥. ما تحتفظ به ذاكرة كاش Cache Memory من بيانات الموجود عند مزود الخدمة من أدلة المعلومات التي يتم أتحصل عليها من المكافئ للموقع (عبد المطلب، ١٤٢٣هـ).

١٦. البيانات التي يتم الحصول عليها من وسائل التحقيق الفنية الأخرى مثل أدوات الضبط، كبرامج كشف الفيروسات، وأدوات المراجعة Auditing، وأدوات مراقبة المستخدمين للشبكة، وأدوات التنصت على الشبكة، والنسخ الاحتياطي، والأدوات مثل IDS, MNM٤ Windows, Content Management.

١٧. البيانات التي يتم الحصول عليها من أدوات فحص ومراقبة الشبكات كأداة TRACER، وأداة ARP، وأداة NETSTAT. ولأدوات المساعدة بالتحقيق كفك التشفير، وأدوات استرجاع المعلومات من الأقراص التالفة مثل View Disk، وبرامج البحث عن الملفات العادية والمخفية مثلXtreepro gold، والبرامج Windows For Rescue File، وResearch Regnerud لاسترجاع الملفات المحذوفة نهائياً من الحاسب الآلي، والبرامج التي تعكس تهيئة القرص الصلب في الحاسب الآلي Unformatted Program.

١٨. البيانات المخزنة بالملفات المؤقتة Temp، عند ما يقوم الجاني بحفظ النصوص أو حذفها أو نقلها أو نسخها، وحتى ولو أنشأ ملف دون الحفظ ضمن مستند يحفظ في ملفات القرص يتم حفظه كملف مؤقت، ويمكن الحصول عليه في Windowstemp.

٣.٦.٣ مصادر الأدلة

يتم البحث عن جميع أنواع الأدلة في جميع المصادر التي يتوقع المحقق أنها تكون موجودة بها، ولذا تم استعراض لتلك المصادر كمسرح الجريمة، والاستجواب، والمعاينة، والتحري، والمرشدين، وأهل الخبرة، والتفتيش، كالتالي:

١. **مسرح الجريمة**

أ. **مسرح تقليدي**: ويقصد الباحث به مسرح الجريمة الذي يقع خارج بيئة الحاسب الآلي والتي يكون الجاني وصلها عند ارتكاب جريمته بهدف الحصول على أدلة مادية، حيث يتوجب على المحقق بالمكان الذي حدثت به الجريمة شاملاً كل ما يمكن أن تصل إليه الأدلة والتي توجد به كالآثار المادية المتخلفة من الجاني بمركز الحاسب الآلي، وأثار استخدامه للأجهزة. كالأوراق، والأقراص المرنة والصلبة، وأشرطة تخزين المعلومات، وجميع القطع الإلكترونية، وأجهزة المودم، والبرامج المستخدمة، والطابعات (داود، ب، ٢٠٠٠م: ٢٢٥)، وأقراص الليزر، والبطاقات المستخدمة في البرامج اللينة، والبطاقات الائتمانية، والشرائط الممغنطة ووسائط الحفظ (البشري، ١٤٢١هـ: ١٩١).

ب. **مسرح إلكتروني**: ويقصد الباحث به مسرح الجريمة الذي يقع داخل بيئة الحاسب الآلي والتي يكون الجاني وصلها عند ارتكاب جريمته سواء باستخدام الجهاز بالوصول المباشر أو الوصول غير المباشر عن طريق شبكة بهدف الحصول على دليل الإلكتروني. فإذا كان المحقق يبحث عن بصمات الجاني وعن بقية الآثار في المسرح التقليدي فإن الجاني يترك بصماته الإلكترونية بمسرح الجريمة الإلكتروني. فالموقع الذي يزوره يفتح سجلاً خاصاً عن معلومات المتصفح كاسمه، والمكان الذي يتصل منه، وعنوان بريده الإلكتروني، واسمه الحقيقي. ولمعرفة ما هي المعلومات التي يسجلها الموقع عن الزائر فموقع www.consumer.net/analyz يوضح ذلك. ويظن بعض الجناة أن استخدام أسماء مستعارة أو استخدام برامج إخفاء الهوية مثل Ghost Mail، قد يخفي جميع معلوماته بشكل كامل، فالجهة الوسيطة ISP التي تقدم الخدمة تحتفظ بسجل عن كافة تحركاته وقيامه بأعمال غير مشروعة كرسائل التهديد أو القنابل البريدية أو التصرفات المخالفة للقوانين والتشريعات المعمول بها. وتفيد تلك المعلومات الجهات الأمنية في التقصي والبحث عن أدلة في نطاق الضبطية القضائية (عبد المطلب، ١٤٢١هـ: ٧٧).

٢. الاستجواب

يتميز استجواب ذوي العلاقة بالحاسب الآلي بأن لديهم المعرفة التخصصية والمهارات الفنية في الحاسب الآلي، وكذلك لهم مصطلحاتهم العلمية التي أصبحت وسيلة التخاطب بينهم. وغالباً تأخذ الاختصارات Acronyms طابعاً لها مثل مصطلح ذاكرة الوصول العشوائية يكونRandom Access Memory ويكون اختصاره RAM فيحتاج استجوابهم إلى معرفة المصطلحات المهمة والاختصارات، والإلمام بعلوم الحاسب الآلي، والتنسيق مع الخبراء في مجال الحاسب الآلي، ومراعاة الحصول على البيانات وطريقة عرض الدليل بحضور الخبير، لمواجهتهم بالأدلة من أجل الحصول على الاعتراف. كما يجب على المحقق الاطلاع على السياسة الأمنية، ومراعاة القانون ومدى ما هو المسموح به والمحدد من سلطة التحقيق (البشري، ١٤٢١هـ: ٣٧٨). ويتم البدء بالمبلغ، ثم الشهود، ثم بالمتهم الأقل تهمة والانتهاء بالمتهم الرئيسي، أو حسب ما يراه المحقق (عبد الحميد، ١٤٢٠هـ: ٢٩٥).

٣. التحري

هي ما يجريه المحقق من محادثات ومقابلات في مكان وقوع الجريمة، وما يجمعه من معلومات عن الأماكن. ولما كانت الجريمة كظاهرة اجتماعية لا يمكن إخضاع أسباب وقوعها لحصر مسبق، فإن مجالات التحري أيضاً لا يمكن إخضاعها إلى حصر مطلق (عبد الحميد، ١٤٢٠هـ: ١٩٣). كما يمكن استخدام شبكة الإنترنت من قبل رجال الأمن بتحري، ففي المنتديات يتفاخرون الجناة بشرح ارتكابهم للجريمة، ونشر تلك الأعمال التي يقومون بها.

٤. المرشدين

يمثل العاملين بالمؤسسات حالياً أو السابقين الذين تم إنهاء خدماتهم لأي سبب والمتخصصين في مجال النظام المعلوماتي، أو المتعاملين مع المؤسسات الأخرى، ولديهم معلومات هامة. وكذلك أصحاب محلات بيع البرامج، وأجهزة الحاسبات الآلية وملحقاتها. "يستوجب من المحقق أن يستبق الأحداث ويعمل على توثيق صلته بأصحابها ومديرها والعاملين

فيها ويشغل في هذا المجال حاجتهم إلى تراخيص لمزاولة مهنتهم، وتقديم خدمات وتسهيلات تؤدي إلى تمهيد وتوثيق الصلة معهم وكسب ثقتهم " (عبد الحميد، ١٤٢٠هـ: ٢٠٠).

٥. **الخبراء**

هم من ذوي الاختصاص الجنائي، أو المتخصصين في مجال الحاسب الآلي، والذين حق للمحقق الاستعانة بهم، وتنظم سلطة التحقيق العلاقة بينهم وبين المحقق ويعتبرون مصدر هام من مصادر الأدلة لاستنتاجهم الأدلة وكتابة تقرير حول تحليل الآثار (عبد الحميد، ١٤٢٠هـ: ٢٨٤).

٦. **المعاينة**

يتم التركيز وتدقيق في وصف المكان الذي يوجد به الحاسب الآلي وملحقاته، وهو ما يطلق عليه تعبير مركز الجريمة وهو المكان الذي يجب أن يشغل جل اهتمام المحقق. وحين يكتشف المحقق أثراً جنائياً، فإنه أما أن يعهد به إلى أحد الخبراء المتخصصين الجنائيين أو المتخصصين في الحاسب الآلي، لرفعه واتخاذ إجراءات مضاهاته مثل بصمات الأصابع التي قد توجد في مركز الحاسب الآلي في حالة كون الجريمة داخلية. وجميع الأدلة المحسوسة كالوراق، والأقراص، وغيرها، ومن ضمن الأشياء التي يجب معاينتها آثار الجريمة الداخلية، والتغيرات التي طرأت على النظام (عبد الحميد، ١٤٢٠هـ: ٢٤٦).

٧. **التفتيش**

يقوم المحقق فور انتهاء تعرفه على الأشخاص المتواجدين داخل المكان بدراسة تقسيمات المكان الداخلية وملحقاته من الأسطح والأفنية والأدوار الأرضية والحدائق، ثم يتولى بعد ذلك رسم خطة تفتيش المكان بحيث يبدأ من نقطة محددة ويتابع تفتيش النقاط التالية بحيث يعود مرة أخرى إلى النقطة التي بدأ منها حتى لا يغفل أي جزء من المكان دون تفتيش، وخلال علية تفتيش أجزاء المكان يجب على القائم بالتفتيش تحري الدقة التامة في إتمام علمية التفتيش والتدقيق في فحص كافة الزوايا والفجوات، وجميع الأمكنة الممكن وجود بها دليل أو أثر (عبد الحميد، ١٤٢٠هـ: ٢٦٠).

٣-٦-٤ حماية الأدلة الإلكترونية

يتواجد الدليل الإلكتروني بمسرح الجريمة الإلكتروني، ولذا يحتاج إلى حماية من أي تغيير قد يحدث بعد الجريمة يسبب إزالة لآثار التي لها دور كبير في اكتشاف الجاني (إنترنت العالم العربي، ١٤٢٣هـ). كما يجب على المحقق أخذ الحيطة والحذر عند المحافظة على الأدلة، فقد يكون التوقيت الذي تم فيه الوصول إلى الملفات دليلاً قوياً وتتصبح الحاجة للسجلات التي ستظهر من هو آخر شخص وصل إلى تلك الملفات أمر مهم، فبالتالي يجب عدم فتح الملف لقراءته، لأن نظام التشغيل يقوم بتغيير تاريخ آخر قراءة للملف لنفس التاريخ الذي قام فيه المحقق بفتح الملف، وهذا بالطبع فيه إزالة لدليل قد يكون له الدور الكبير في اكتشاف الجاني. ولذا عليه استخدام أداة تساعد في حماية مسرح الجريمة، كاستخدام الأدوات التي قامت إحدى المؤسسات المتخصصة في مجال أمن المعلومات في الإنترنت بإنتاجها والتي تمنع الكتابة للقرص الصلب بعد عملية جريمة الاختراق، بحيث تبقى المعلومات كما هي (الطويل، ١٤٢٣هـ: ١٨). فعند توثيقه يجب حفظه أو حفظ نسخه منه في أدوات حفظ خارجية وكتابة البيانات الهامة عليها كالوقت والتاريخ وأسم الشخص الذي توصل إلى الدليل وأنوع نظام التشغيل واسم البرنامج والمعلومات المتضمنة (البشري، ١٤٢٣هـ: ٩٧).

٣-٧ خلاصة الفصل الثالث

تناول هذا الفصل أمن نظم المعلومات والسياسات الأمنية، حيث تم التطرق إلى التحديات التي يجب أخذها في الحسبان لضمان مستوى مناسب من أمن المعلومات. كما تم التطرق إلى الإجراءات الإدارية والفنية لأمن المعلومات. أما في السياسة الأمنية فتم التطرق إلى متطلبات تصميم السياسة الأمنية، وخصائصها، ومكوناتها. وفي جرائم نظم المعلومات تناول الباحث أنماط جرائم نظم المعلومات وأساليب وأدوات ارتكابها. وأما في وسائل التحقيق جرائم نظم المعلومات تم تناول وسائل التحقيق المادية والإجرائية. كما تناول الباحث الأدلة المثبتة وأنواعها ومصادرها. وعوائق التحقيق.

الفصل الرابع/ الدراسات السابقة

٤-١ المقدمة

أظهرت مراجعة الدراسات السابقة في الدوريات العلمية المحكمة، والرسائل الجامعية في كل من (مكتبة الملك عبد العزيز العامة، ومكتبة الملك فهد الوطنية، ومدينة الملك عبد العزيز للعلوم والتقنية، وأكاديمية نايف العربية للعلوم الأمنية، وجامعة الملك سعود، وجامعة الإمام محمد بن سعود الإسلامية، ومعهد الإدارة العامة، والمواقع المتخصصة على شبكة الإنترنت التي تعني بهذا النوع من الجرائم ووسائل اكتشافها) عدم وجود دراسة تناولت وسائل التحقيق في مجال جرائم نظم المعلومات، أو أجريت على نفس مجتمع الدراسة، ولذا تم اختيار الدراسات ذات العلاقة بموضوع الدراسة أو بأحد عناصرها.

٤-٢ الدراسات العربية

استعرض فيه الباحث (١٦) دراسة عربية وفق ترتيب تنازلي حيث بداء بدراسات التي أجريت (١٤٢٤هـ، ٢٠٠٣م) وانتهى بدراسات التي أجريت في عام (١٤١٣هـ، ١٩٩٢م)، على النحو التالي:

١. دراسة (المنشاوي، ١٤٢٤هـ).

أجريت حول "جرائم الإنترنت في المجتمع السعودي" وعينتها جميع مستخدمي الإنترنت في المملكة. وبينت نتائجها حجم ارتكاب مستخدمي الإنترنت في المجتمع السعودي للجرائم الجنسية والممارسات غير الأخلاقية، بحيث أظهرت نسبة ارتياد المواقع الجنسية بأنها (٤٤,٨٪) والذين يطلبون مواد جنسية تبلغ نسبتهم (١٥,٤٪)، والمشتركين بقوائم جنسية تبلغ نسبتهم (١٤,٩٪)، والذين ينشئون مواقع جنسية تبلغ نسبتهم (١,٢٪)، والذين ينشئون قوائم بريدية جنسية تبلغ نسبتهم

(٢,٩٪)، أما الذين يقومون بالتشهير بالآخرين تبلغ نسبتهم (١,٧٪)، كما يتم اجتياز البروكسي بنسبة (٣٥,٤٪) من عدد المستخدمين، كما تبلغ نسبة من يستخدمون برامج إخفاء الشخصية أثناء تصفح الإنترنت (١٣,٥٪)، ويتم استخدام برامج إخفاء الشخصية أثناء إرسال البريد الإلكتروني من قبلهم بنسبة (٨,٨٪)، كما يتم انتحال شخصية الآخرين أثناء التصفح أو إرسال البريد الإلكتروني بنسبة (٨,٨٪).

٢. دراسة (الجهني، ١٤٢٣هـ).

أجريت هذه الدراسة حول "اتجاهات العاملين في الأجهزة الأمنية نحو أهمية استخدام البريد الإلكتروني وحماية المعلومات" دراسة مسحية على مركز المعلومات الوطني بالرياض. ومن أبرز نتائجها أن البريد الإلكتروني يساهم في الحصول على معلومات سريعة عن المطلوبين للعدالة وإنجاز الأعمال في أي وقت ومن أي مكان (الجهني، ١٤٢٣هـ). كما بينت الدراسة أن هناك معوقات تحول دون استخدام البريد الإلكتروني منها الخوف من إرسال فيروسات عن طريقة، أو يتم اختراقه أو تحريف المعلومات المرسلة، كما أن التوسع في استخدامه مع وجود ضوابط لحماية المعلومات المرسلة يؤدي إلى خفض التكاليف مما يسهم في ترشيد النفقات.

٣. دراسة (النفيعي، ١٤٢٣هـ)

أجريت حول "مقاهي الإنترنت والانحراف إلى الجريمة بين مرتاديها" دراسة تطبيقية على مرتادي مقاهي الإنترنت بالمنطقة الشرقية. وشملت الدراسة ثلاث عينات من مستخدمي الإنترنت فالأولى الذين يرتادوا المقاهي، والثانية الموقوفين بإصلاحية الدمام (البالغين الأكثر من ١٨ سنة)، والثالثة الموقوفين بدار الملاحظة الاجتماعية بالدمام (الأحداث الأقل من ١٨ سنة)، ومن أبرز نتائجها أن أغلب أفراد عينة الدراسة من مرتادي المقاهي هم فئة الشباب الأقل من (٣٠) سنة، ومن ذوي المستوى التعليمي المرتفع (ثانوي فما فوق)، وغالبيتهم من الموظفين، كما أدلى غالبيتهم أن أكثر خدمات الإنترنت استخداماً مجموعة الدردشة، ومن ثم الرسائل الشخصية عبر خدمة البريد

الإلكتروني، وأظهرت أن هناك عوامل تجذبهم إلى المقاهي من أبرزها اكتساب للعديد من المعلومات، كما أن الفراغ والتسلية من أكثر تلك العوامل الأخرى التي تجبهم. كما أوضحت وجود آثار سلبية كبيرة للتعامل مع الإنترنت في المقاهي على الانحراف السلوكي للمرتادين كان على رأسها وجود روابط في العلاقات عبر الإنترنت قد تؤدي إلى علاقات غير شرعية بين الجنسين.

٤. دراسة (البشري، ١٤٢٣هـ).

عنوانها "الأدلة الجنائية الرقمية: مفهومها ودورها بالإثبات" ومن أهم ما ذكر فيها أن الأدلة الرقمية تختلف عن الأدلة الجنائية الأخرى في علاقتها بالأسلوب الإجرامي وطرق جمعها ومن يقوم بها، وتصنيفها، وتناول إسهامات ذلك نوع من الأدلة في الإثبات الجنائي وحجيتها. وأظهرت نتائج دراسته أن الأدلة الرقمية أكثر الأدلة وفرة وثباتاً، وأنها نالت مصداقية أمام المحاكم المدينة والشرعية، وأن الأجهزة الرقمية التي تفحص الأدلة المادية كالبصمات الوراثية أولى بفحص الأدلة الرقمية.

٥. دراسة (الهاجري، ١٤٢٣هـ).

عنونها "الحرب المعلوماتية" وذكر فيها أنه مع ظهور الحاسب الآلي واستخدام شبكات لربط أجهزة الحاسب وانتشار شبكة الإنترنت بشكل خاص واتساع استخدامها، أخذت حرب المعلومات بعداً جديداً، فالتضخم الكبير في صناعة المعلومات جعل الاعتماد على النظم أكبر وأكثر في إدارة أمور الحياة المختلفة ولذا فإن استخدام المعلومات كسلاح أصبح أكثر عنفاً و أشد تأثيراً. وذكر أن هناك ثلاثة عناصر أساسية للحرب المعلوماتية هي المهاجم والمدافع والمعلومات ونظمها.

٦. دراسة (الشهري، ١٤٢٢هـ).

أجريت حول "المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي" دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، (الشهري، ١٤٢٢هـ) بين في دراسته أن

جرائم الحاسب الآلي من أخطر الجرائم التي تقع على نظم المعلومات، لكون المؤسسات تعتمد بشكل متزايد على نظم المعلومات وأنها في تزايد، وطبق دراسته على عينة عشوائية مكونة من (٣٠٢) مفردة بحث، ومن أهم نتائجها أن هناك معرفة وأدراك لهذا النوع من الجرائم من قبل العاملين بالأجهزة الأمنية، حيث أفاد ما نسبته (٧٩,١٪) منهم بمعرفتهم بهذه الجرائم، كما أظهرت دراسته أن جرائم الحاسب الآلي ليست منتشرة في جميع منطقة الرياض بشكل كبير حيث أفاد (٨٩,٤٪)، منهم بعدم تلقيه البلاغ عن تلك الجرائم، كما أفاد (٩٤,٧٪)، بعدم مشاركتهم بالتحقيق، كما أظهرت عدد من المعوقات الإدارية في التعامل الأمني أن أهمها نقص المعرفة بالحاسب الآلي إذ بلغ المتوسط (٤,٦١) ونقص مهارات التعامل مع الإنترنت (٤,٣٩) وعدم كفاية التدريب، وعدم توفير الاتصال بالإنترنت، وعدم توفر أجهزة حاسب، والخبراء، كما يدخل من ضمن تلك المعوقات عدم الإبلاغ عن الجريمة (٣,٥١)، ونقص الأنظمة المجرمة لها (٣,٨٧)، ووضحت دراسته أن هناك فرق ذي دلالة إحصائية بين المؤهل العلمي والمعرفة بالجرائم لصالح المؤهل العلمي العالي.

٧. دراسة (الهاجري، ١٤٢٢هـ).

تحمل عنوان "جرائم الإنترنت" تناول فيها أهم الأهداف المقصودة في تلك الجرائم وحددها بالمعلومات وتشمل سرقتها أو تغييرها أو حذفها، وأما الأجهزة وتشمل تعطيلها أو تخريبها، أما الأشخاص أو الجهات وتستهدف فئة كبيرة من الأشخاص أو الجهات على شبكة الإنترنت بشكل مباشر كالتهديد أو الابتزاز. وقد أستعرض عددٍ من الجرائم كصناعة ونشر الفيروسات، والاختراقات وذكر أنها تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي. إن جل عمليات الاختراقات (أو محاولات الاختراقات) تتم من خلال برامج متوفرة على الإنترنت يمكن لمن لديه خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة غير، وهنا تكمن الخطورة. ومن ضمن الجرائم التي استعرضها تشويه المواقع Defacing، وتعطيل الأجهزة، وانتحال

الشخصية، المضايقة والملاحقة، والتغرير والاستدراج، والتشهير وتشويه السمعة، والتغرير والاستدراج، وصناعة ونشر الإباحية، والنصب والاحتيال.

٨. دراسة (البشري) في عام ١٤٢١هـ

تتعلق "بالتحقيق في جرائم الحاسب الآلي والإنترنت" وهي دراسة وصفية مكتبيه وتهدف إلى نقل اهتمام الكِتابّ، والمحققين، والعاملين في مجال المهن الأمنية إلى نوع جديد من التحقيقات الجنائية التي تتطلبها متغيرات جرائم الألفية الثالثة المحتمل أن تكون مسارحها خارج مسارح الجريمة التي ألفناها وأساليب غير الأساليب المعهودة. وذكر من الصعوبات التي تواجه المحققين ورجال الشرطة عند التصدي لجرائم الحاسب الآلي قصور التشريعات التي تجرم جرائم الحاسب الآلي بسبب التطورات السريعة في تقنية الحاسب الآلي.واحتوت الدراسة على تعريف المفردات الضرورية المتعلقة بأركان جرائم الحاسب الآلي، وتصنيفها، وأنواعها، وكيفية ضبطها، تم تناول إجراءات التحقيق في جرائم الحاسب الآلي التي تتميز ببعض الخصوصية في عناصر التحقيق الفرعية والإجراءات الشكلية المتبعة في تلقي البلاغات والعناية بمسرح الجريمة وتكوين فرق العمل، وأساليب تامين الأدلة المادية. وأكدت الدراسة على انه يجب الاستعانة بتقنية الحاسب الآلي للتحقيق في جرائم الحاسب الآلي وبمتخصصين في علوم الحاسب الآلي (البشري، ١٤٢١هـ).

٩. دراسة (المسند، والمهيني، ١٤٢١هـ).

في دراسة (المسند، والمهيني) حول "جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات" تناولت بشكل عام في دراسة وصفية مكتبيه تعريف جرائم الحاسب الآلي، وأنواعها، و أثرها على المجتمع وأساليب مكافحتها. وذكرت الدراسة أن جرائم الحاسب الآلي مع وجود دعم الإنترنت وانتشارها السريع بهذا الشكل قد تمثل تهديداً مباشراً وفورياً وسريعاً للأمن الوطني والاقتصاد المحلي والعالمي، وانتهاكاً لحقوق الأفراد والمؤسسات على اختلاف أنواعها، وقد وجد المتسللون والمتطفلون ومحترفو الجرائم ضالتهم في الشبكة العالمية لممارسة جرائم التزوير

واختلاس الأموال والقرصنة المعلوماتية، والتجسس (المسند، والمهيني، ١٤٢١هـ). ومما أظهرته هذه الدراسة، انه يصعب اكتشاف جرائم الحاسب الآلي لأنه لا يوجد في الغالب شاهد للقضية أو أدلة يمكن استخدامها لتوصل إلى الجاني، وأن أكثر المنشآت تتكتم على ما يحدث لنظمها من اختراقات حيث تشير الإحصائيات إلى أن (١١٪) هو ما يتم الإبلاغ عنه، كما أن هنالك أسباب للاهتمام بجرائم الحاسب الآلي وهو أن كثير من المؤسسات الإدارية أصبحت تعتمد على نظم المعلومات بشكل مطرد، وهذه الجرائم تعرض نشاطها للتعطل الجزئي أو الكلي بالإضافة إلى أن ظهور شبكة الإنترنت جعل من تلك المؤسسات الإدارية تقوم بإنشاء لها مواقع على هذه الشبكة عارضين معلوماتهم للزائرين، ويقابل ذلك نقص المعلومات عن أدوات الحماية المتاحة لنظم المعلومات. ومن توصيات هذه الدراسة تعزيز التعاون الدولي والإقليمي في قضايا جرائم الحاسب الآلي بإنشاء أقسام متخصصة للتحقيق في هذه النوعية من الجرائم، وقاعدة بينات تتضمن وصفاً لجرائم الحاسب الآلي.

١٠. دراسة (بحر، ١٤٢٠هـ).

أجراها حول "معوقات التحقيق قي جرائم الإنترنت" وهي دراسة مسحية على ضباط الشرطة في دولة البحرين وهدفت هذه الدراسة إلى الكشف عن معوقات التحقيق قي جرائم الإنترنت بوجه عام. وتلخصت أهم النتائج، أن المعوقات الشخصية تمثل عائقاً للتحقيق في جرائم الإنترنت لدى (٦٣,٣٪)، من العينة، ولقد أجمع أكثر من ثلثي العينة بأن المعوقات الفنية والإدارية تمثل عائق أمام التحقيق في تلك الجرائم، وتمثل المعوقات التشريعية عائقاً لتحقيق في جرائم الإنترنت لدى ما يقارب ربع العينة، وأظهرت نتائج الدراسة وجود معوق عدم متابعة المستجدات في مجال جرائم الإنترنت كأبرز معوق شخصي لدى ضباط الشرطة، كما أظهرت نتائج الدراسة وجود العديد من المعوقات الفنية، كمعوق عدم كفاية المعرفة لاستخدام الحاسب الآلي والإنترنت و معوق عدم كفاية المعرفة لمصطلحات الحاسب الآلي والإنترنت و معوق عدم كفاية المعرفة لأساليب ارتكاب جرائم الإنترنت و معوق عدم كفاية الخبرة للتحقيق في مجال جرائم الإنترنت ومعوق عدم كفاية

المعرفة باللغة الإنجليزية لدى ضباط الشرطة، كما أظهرت نتائج الدراسة وجود معوقات إدارية كمعوق عدم توفير الدورات التخصيصية للتحقيق في جرائم الحاسب الآلي والإنترنت، وكذلك معوق عدم توفير خدمة الاتصال بالإنترنت، وأظهرت نتائج الدراسة وجود معوقات تشريعية، كمعوق عدم كفاية التشريعات المحلية والدولية ومعوق عدم كفاية المعرفة بالتشريعات لدى ضباط الشرطة.

١١. دراسة (النويصر، ١٤١٩هـ).

أجرها حول "دور نظم المعلومات في مكافحة الإرهاب" وهي دراسة تطبيقية على بعض الأجهزة الأمنية في المملكة والتي تهدف دراسته إلى التعرف على نظم المعلومات وأنواعها، وخصائصها، ومكوناتها والتعرف على وظائفها ودورها في مكافحة الإرهاب، وكيفية تأمين المعلومات ودورها في اتخاذ القرارات، والتعرف على جوانب القصور في نظم المعلومات الأمنية، ودورها في اتخاذ القرارات الأمنية وعلاقتها بنظام الاتصالات. ومن أبرز النتائج التي توصلت إليها الدراسة أنها أكدت على أهمية نظم المعلومات وأن أهم القصور عدم توفر برامج تدريبية على الحاسب، وعدم وجود أجهزة كافية، وعدم وجود برامج مناسبة وعدم توفر قاعدة بيانات جيدة.

١٢. دراسة (السحيباني، ١٤١٧هـ).

أجراها حول "كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات" وهي دراسة مسحية شملت عدد من البنوك في المملكة. وتناولت الدراسة أهمية المحافظة على أمن المعلومات وخصوصاً التي يكون موضوعها الحاسب الآلي وهدفت هذه الدراسة إلى الكشف عن الإجراءات الإدارية المستخدمة في البنوك للمحافظة على المعلومات ومعرفة جوانب القوة في الإجراءات الأمنية المعمول بها حالياً بالبنوك، وعلى مستوى الحماية. وتناولت في إطارها النظري أمن المعلومات التي يكون موضوعها الحاسب الآلي والأخطار التي تهدد أمنها والتي تحدث بفعل الإنسان والذي يهدف بفعله الدراسة إلى النيل من معلومات المؤسسات الإدارية عن طريق الحاسبات الآلية بغرض الحصول عليها أو تغييرها، أو تعديلها، أو إتلافها كلياً لتحقيق مكاسب غير مشروعة

ومن ابرز نتائج هذه الدراسة أيضاً عدم وجود فروق ذات دلالة إحصائية بين البنوك الأجنبية والعربية والوطنية في الإجراءات الإدارية المتخذة لحماية أمن المعلومات نتيجة لتشابه النشاط. والإجراءات الإدارية المطبقة في البنوك، من الدخول للبنك، غرفة الحاسب الآلي، ووسائط التخزين؛ والاعتماد على حارس الأمن في حراسة البنك لقدرته على حصر الدخول بصاحب الرقم السري أو البطاقات الآلية أو المفاتيح العادية دون أي شخص مصاحب له. كما لا يوجد فروق ذات دلالة إحصائية بين الإجراءات الإدارية المطبقة في البنوك وعملية تصميم برامج شبكة الاتصالات والبرامج على مبرمجين من داخل البنوك وليس متعاونين من خارجها، وهذا أجراء عال الكفاءة، كما لا يوجد فرق ذو دلالة إحصائية بين الإجراءات الإدارية المطبقة في البنوك وعملية تصميم برامج شبكة الاتصالات بأسلوب يضمن استمرارها. كما بينت الدراسة عدم وجود فروق ذات دلالة إحصائية بين الإجراءات الإدارية المطبقة في البنوك وعملية التحري عن الموظف لما يمثله الموظف المشبوه من تهديد لأمن معلوماتها وخاصة المبرمجين والعاملين بأمن المعلومات. لإجراءات الأمنية المطبقة في البنوك وعملية وجود رقابة أمنية على إدخال ومخرجات الحاسب الآلي من أوراق، وتقارير، وأشرطة ممغنطة وإجراءات أتلاف منتهى الصلاحية حتى لا يتم الاستفادة منها وقد وقعت بعض الجرائم التي تؤكد ذلك.

١٣. الحلقة العلمية (شرطة دبي، ١٩٩٦م).

ناقشت الحلقة العلمية والتي بعنوان "الإنترنت من منظور آمني" والمنعقدة في قيادة شرطة دبي في عام ١٩٩٦م. أوصت بعقد دورات تخصصية لضباط الشرطة لتعريفهم بأساليب البحث والتحري في شبكة الإنترنت.

١٤. دراسة (رستم، ١٩٩٤م).

هي دراسة مقارنة كان عنوانها "الجوانب الإجرائية للجرائم المعلوماتية" وتناولت موضوع التحقيق في الجرائم المعلوماتية والصعوبات التي تواجه التحقيق فيها، وذكر من أسباب الصعوبات

التي تواجه التحقيق في الجرائم المعلوماتية نقص خبرة وتدريب الشرطة لمواجهة تلك الجرائم، وأن المتدرب لتحقيق في تلك الجرائم لابد من توفر لدية المعرفة العلمية والقدرات الذهنية والنفسية، لتلقي التدريب، وتطرقت إلى موضوع التدريب التخصصي، ومقومات الخبرة الفنية والعلمية في مجال الجرائم المعلوماتية (رستم، ١٩٩٤م).

١٥. دراسة (عوض، ١٩٩٣م).

كانت تحت عنوان "جرائم نظم المعلومات" تناول في دراسته جرائم نظم المعلومات والمشكلات القانونية المصاحبة لجرائم الحاسب في القوانين الجنائية، وذكر في دراسته تقرير المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة في أكتوبر عام ١٩٩٣م أن من توصيات المؤتمر بان هناك حاجة ماسة لتدريب رجال الشرطة، ورجال التحقيق، ورجال القضاء ليكونوا على معرفة ودراية بالناحية الفنية للمعلوماتية.

١٦. دراسة (قشقوش، ١٩٩٢م).

تتعلق "بجرائم الحاسب الإلكتروني في التشريعات المقارنة" ذكرت أن هناك نقص في النصوص التشريعية بخصوص الجرائم المعلوماتية وأن هناك صعوبات في تطبيق النصوص التقليدية المعمول بها في قوانين العقوبات على تلك الجرائم المستحدثة، وأن هناك صعوبات في الإثبات الجنائي لتلك الجرائم تواجه المحققين فيها، وتطرق إلى طرق ارتكاب الجرائم المعلوماتية، وتحليل طبيعتها، ثم تعرضت لذكر أهم أنواع الجرائم المعلوماتية كسرقة وتخريب المعلومات الموجودة بالحاسب الآلي وموقف النصوص التشريعية منها.

٣-٤ الدراسات الأجنبية

استعرض الباحث (٥) دراسات أجنبية أجريت خلال الفترة ما بين (٢٠٠٢م) حتى عام (١٩٧٨م). وقد استعرضها الباحث وفق ترتيب تنازلي، وكانت على النحو التالي:

١. **دراسة (Rapalus. ٢٠٠٢).**

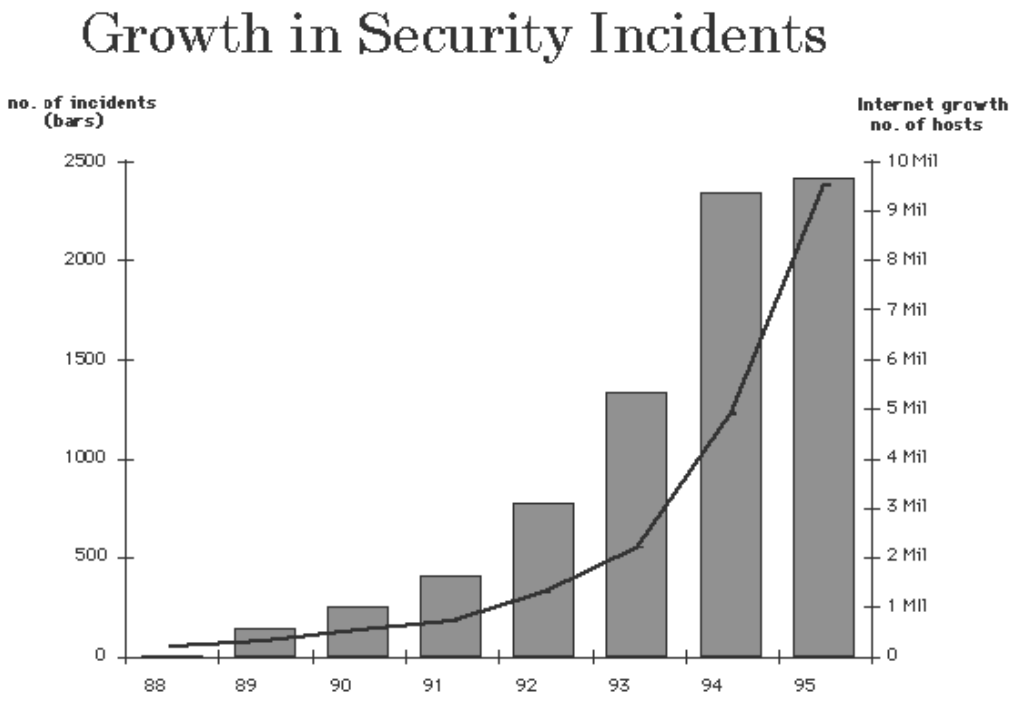
حول "جنيات أمن المعلومات" (Information Security Breaches)، نشرها معهد أمن الحاسب الآلي Computer Security Institute في شهر أبريل من عام ٢٠٠٢م بالتعاون مع مكتب التحقيقات الفيدرالية (F B I) حول جرائم نظم المعلومات، شارك فيها أكثر من (٥٠٣) مسؤول من أمن المعلومات وأفادت الدراسة أن مؤسسات الأعمال الأميركية تتكبد خسائر مالية متزايدة نتيجة لمخالفات وجنايات أمن المعلومات، وأفادت أن نسبة (٩٠٪) من المجيبين (وغالبيتهم من المؤسسات الكبرى والهيئات الحكومية) اكتشفوا مخالفات أمنية لحاسباتهم الآلية، وأن نسبة (٨٠٪) اعترفوا بخسائر مالية، كما أن عدد (٢٢٣) فرداً من العينة ما يمثل نسبة (٤٤٪) منهم أفادوا عن خسائر بقيمة (٤٥٥،٨٤٨،٠٠٠) دولار، مقارنة بـ: (٣٧٨) مليون دولار تقريباً بلغ عنها (١٦٨) فرداً عام ٢٠٠١م، ومقارنة بـ: (٢٦٥) مليون دولار بلغ عنها (٢٥٠) شخصا استطلعت آراؤهم في عام ٢٠٠٠م، كما أن متوسط الخسارة السنوية على مدى ثلاث سنوات قبل عام ٢٠٠٠م كان في حدود (١٣٠) مليون دولار كما أفادت الدراسة أن (٩١٪) اكتشفوا إساءة استخدام موظفين لديهم لشبكة الإنترنت مثل الاتصال بموقع لصور إباحية ولبرمجيات قرصنة وطباعة محتوياتها أو استخدام غير لائق لنظم البريد الإلكتروني، وأن (١٣٪) أبلغوا عن سرقة معلومات أو بيانات تتعلق بمعاملات تجارية، (٤٠٪) اكتشفوا أن النظام المعلوماتي لديهم قد تم اختراقه من الخارج, وأن (٩٨٪) منهم يملكون موقع على الشبكة العنكبوتية، كما أفادت الدراسة أن هناك زيادة في جرائم نظم المعلومات في عام ٢٠٠١م أكثر من عام ٢٠٠٠م، حيث أن (٩٤٪) اكتشفوا فيروسات حاسب آلي مقارنة بـ: (٨٥٪) في عام ٢٠٠٠م، ونسبة (٩٠٪) منهم ابلغوا عن عمليات تخريب مقابل (٦٤٪) في ٢٠٠٠م، ونسبة (٨٪) ابلغوا عن حالات احتيال أو تزوير مالي مقابل ونسبة (٣٪) في ٢٠٠٠م.

٢. **دراسة (CERT, B, ٢٠٠٢).**

أظهرت دراسة منظمة طوارئ الحاسب الآلي (Computer Emergency Response (CERT Team والتي كانت عن "نمو المخالفات والإنترنت Incidents & Internet Growth" أنه كلما زادت

الحاجة لاستخدام نظم المعلومات زاد معدلات عدد المستخدمين للإنترنت، وبتالي يكون هناك ازدياد طردي مرافق في معدلات ارتكاب الجرائم عن طريقها، فمنذ إنشاء تلك المنظمة عام ١٩٨٨م لاحظت أن الجرائم تزداد بازدياد عدد المشتركين في الإنترنت فكانت أقل من (١٠٠) حادثة عام ١٩٨٨م وأكثر من (٢٥٠٠) جريمة عام ١٩٩٥م. كما في شكل رقم (٧).

شكل رقم (٧) زيادة الجرائم مع تزايد عدد المشتركين في الإنترنت



المصدر: (CERT,B, ٢٠٠٢)

٣. دراسة (Wahbler,١٩٩٨)

أظهرت هذه الدراسة (Wahlbert) التي كانت عن "جرائم الحاسب الآلي Computer Crime" بشكل عام تعد من أكبر التحديات التي تواجه أجهزة التحقيق والقضاء في استراليا، وأن قطاع كبير من المحققين قليلي الخبرة يواجهون صعوبات فنية وعملية للحصول على أدلة كافية للإدانة في هذه الجرائم، وأظهرت هذه الدراسة بأن أغلب المدانين في هذه الجرائم هم من ذوي المهارات الفنية في استخدام الحاسب الآلي.

٤. **دراسة (Tim, ١٩٩٨).**

أبرزت هذه الدراسة التي تحمل عنوان "جرائم الحاسب الآلي Computer Crime" والتي نشرها معهد أمن الحاسب الآلي Computer Security Institute بالتعاون مع مكتب التحقيقات الفيدرالية (F B I) أن (٥٢٠) شركة أمريكية أبلغت عن فقدان ما قيمته (١٢٠) مليون دولار بسبب جرائم الحاسب في عام ١٩٩٧م أي بزيادة عن عام ١٩٩٦م بنسبة (٣٦٪)، وأن (٥٤٪) من المشمولين بالدراسة يرون أن مؤسساتهم كانت هدفاً للاختراق بواسطة الإنترنت.

٥. **دراسة (Bequai, ١٩٧٨).**

أوضحت دراسة بكوي (Bequai) أن التدريب على التحقيق في جرائم الحاسب الآلي يجب أن يكون من الأولويات في أجهزة الشرطة، فالحاجة لهذا التطوير والتدريب لرجال الأمن في مجال التحقيق في جرائم الحاسب الآلي مهم لمواجهة مثل هذه الجرائم

٤ـ٤ التعقيب على الدراسات السابقة

في دراسة (المنشاوي) حول "جرائم الإنترنت في المجتمع السعودي" ركزت على الجرائم وخصوصاً الجرائم على العنصر البشري، ولم تركز على الجرائم التي تقع على المعلومات والأجهزة، ولم يتطرق إلى التحقيق، وتشابه دراستي من ناحية أنها بينت حجم بعض الجرائم في المجتمع السعودي ولكنها بشكل عام حيث أن دراستي تركز على الجرائم بشكل خاص والتي تتعرض لها بعض المؤسسات. أما دراسة (الجهني) في عام ١٤٢٣هـ، والتي هي حول "اتجاهات العاملين في الأجهزة الأمنية نحو أهمية استخدام البريد الإلكتروني وحماية المعلومات" أوضحت أن هناك معوقات تحول دون استخدام البريد الإلكتروني منها الخوف من إرسال فيروسات عن طريقة، أو يتم اختراقه أو تحريف المعلومات المرسلة وهذا يوضح مدى وعيهم بجرائم نظم المعلومات، وفي دراسة (الشهري) حول "المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي: دراسة

مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض" تشابه دراستي من ناحية التطرق للجرائم ومعرفة التعامل الأمني من قبل الجهات الأمنية ولكن تختلف بأنها لم تتطرق إلى وسائل التحقيق ولم تتطرق إلى كافة المعوقات وتطرقت فقط لمعوقات التعامل من الناحية الإدارية.

وفي دراسة كل من (المسند، والمهيني) حول "جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات" ودراسة (قشقوش) والمتعلقة "بجرائم الحاسب الإلكتروني في التشريعات المقارنة" توافقان دراستي من ناحية المعرفة بجرائم الحاسب باعتبار أن جرائم نظم المعلومات جزءاً من جرائم الحاسب، وركزت تلك الدراسات على معرفة جرائم الحاسب الآلي وأساليب ارتكابها. ولكنها لم تتطرق إلى وسائل التحقيق في جرائم نظم المعلومات. وأما وفي دراسة (البشري) والمتعلقة "بالتحقيق في جرائم الحاسب الآلي والإنترنت" فإنها كذلك توافق دراستي من ناحية المعرفة في جرائم الحاسب باعتبار أن جرائم نظم المعلومات جزءاً من جرائم الحاسب وأيضاً التحقيق في تلك الجرائم بالرغم أنها لم تتطرق إلى وسائل التحقيق.

وأما في دراسة (بحر) في "معوقات التحقيق قي جرائم الإنترنت" وهي دراسة مسحية على ضباط الشرطة في دولة البحرين تتفق مع دراستي في معرفة جرائم الإنترنت وأساليب ارتكابها بدراسة وصفية ومعوقات التحقيق جرائم الإنترنت. ولكنها اكتفت بالبحث عن المعوقات. ولم تتطرق إلى وسائل التحقيق في جرائم نظم المعلومات. وفي دراسة كل من(عوض) عن "جرائم نظم المعلومات" ودراسة (رستم) "المتعلقة بالجوانب الإجرائية للجرائم المعلوماتية" ودراسة كل من (Tim) و(Rapalus) التي نشرها معهد أمن المعلومات Computer Security Institute تبين حجم الجرائم المتزايدة والتي بينت ارتفاع في السنوات الأخيرة، وتوافق دراستي من ناحية الاطلاع على حجم الجرائم ونوعيتها، ومدى أضرارها، ولكن تختلف من ناحية عدم التطرق إلى وسائل التحقيق. أما دراسة بكوي (Bequai) ودراسة والبرت (Wahlbert) تناولت هذه الدراسات موضوع التحقيق

في الجرائم المعلوماتية من ناحية معرفة الصعوبات التي تواجه المحققين، ومن ناحية أهمية التدريب لتحقيق في تلك الجرائم ولكنها لم تتطرق إلى وسائل التحقيق في جرائم نظم المعلومات.

وأما دراسة (النويصر) حول "دور نظم المعلومات في مكافحة الإرهاب" ركزت على معرفة نظم المعلومات وسلبياتها وإيجابيتها ولكن لم تتطرق إلى حماية نظم المعلومات من الجرائم والتحقيق فيها. أما دراسة (السحيباني) حول "كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات" ركزت على حماية المعلومات ولم تتطرق إلى أساليب ارتكاب الجرائم ولا إلى التحقيق في هذه الجرائم، كما أثبتت دراسة منظمة CERT أن هناك علاقة طردية بين عدد مستخدمي الإنترنت والجرائم. وبشكل عام تتشابه بعض الدراسات السابقة مع دراسة الباحث الحالية في مجال دراسته، وأن كانت معالجة الدراسات السابقة تختلف عن معالجة الدراسة الحالية لمعرفة وسائل التحقيق في جرائم نظم المعلومات. هذا وسوف يستفيد الباحث من تلك الدارسات السابقة و سيبدأ من حيث انتهت.

٤ـ٥ خلاصة الفصل الرابع

استعرض الباحث (٢١) دراسة عربية وأجنبية حيث أظهرت أغلب الدراسات أن هناك أهمية كبيرة لاستخدام النظم، كما أن هناك تزايد كبير في جرائم النظم وتنوع في أساليبها وأدواتها وأنها ذات طابع خاص يختلف عن الجرائم التقليدية، وأن هناك حاجة إلى المكافحة سواء بقيام الجهات التي يمكن أن تتضرر بحماية معلوماتها، أو بقيام جهات التحقيق بأداء عملها في ظل عنصرين مهمين وهما؛ وجود التشريع، والقدرة على بالتحقيق في هذه الجرائم.

الفصل الخامس/ منهج الدراسة وأسلوبها

٥-١ المقدمة

يتناول هذا الفصل منهج الدراسة، ومصادرها، وتحديد مجتمعها وعينتها، كما يتطرق لبناء أداة الدراسة والخطوات التي تم إتباعها للتحقق من صدقها وثباتها. ويبين أسلوب أجراء الدراسة ميدانياً، وأخيراً يوضح أساليب المعالجة الإحصائية التي تم استخدامها لتحليل البيانات التي تم جمعها.

٥-٢ منهج الدراسة

تعد هذه الدراسة من الدراسات الوصفية والتي تعتمد على دراسة الواقع أو الظاهرة كما توجد في الواقع ويهتم بوصفها وصفاً دقيقاً ويعبر عنها تعبيراً كيفياً وكمياً (عبيدات، وآخرون، ٢٠٠١م). وهو منهج لا يقف عند هذا الحد بل يعمد إلى تحليل الظاهرة وكشف العلاقات بين أبعادها المختلفة من اجل تفسيرها والوصول إلى استنتاجات تسهم في تحسين الواقع وتطويره (العساف، ١٤٢١هـ)، وعلى ضوء طبيعة الدراسة التي ستعالج موضوعاً على قدر كبير من الأهمية من الناحية الأمنية والإدارية والفنية وهو وسائل التحقيق في جرائم نظم المعلومات يستخدم الباحث المنهج المسحي، الذي يعتمد على جمع معلومات موضوع الدراسة من المجتمع.

٥-٣ مصادر الدراسة

اعتمدت الدراسة على المعلومات المستقاة من المراجع والبحوث والدراسات السابقة والنشرات بغرض التعرف على أهم ما كتب عن جرائم نظم المعلومات ووسائل التحقيق فيها، وعلى مواقع شبكة الإنترنت التي تعنى بهذا النوع من الجرائم ووسائل اكتشافها، وعلى ما توفره المؤسسات المنتجة لوسائل أمن المعلومات من أدلة استخدام ووثائق وأدوات. كما قام الباحث

بتصميم استبيان يحتوي على أسئلة الدراسة لمعرفة وجهات نظر وآراء مجتمع الدراسة ومن ثم استخلاص النتائج والمؤشرات بتحليل بياناته.

٥-٤ حدود الدراسة

تقتصر هذه الدراسة على مجتمع الدراسة الذي تم سحب العينة منه فقط، ويتكون من المحققين العاملين في أقسام الشرطة المنتشرة في مدينة الرياض ومنسوبي الشؤون الفنية بوزارة الداخلية، ومن العاملين في مجال نظم المعلومات بالقطاع العام (إدارة التقنية البنكية بمؤسسة النقد العربي السعودي، ومركز المعلومات الوطني، ووحدة خدمات الإنترنت بمدينة الملك عبد العزيز للعلوم والتقنية)، والقطاع الخاص (المؤسسات القابضة، والمؤسسات المساهمة، والمؤسسات الحكومية، والقطاعات المصرفية)، في مدن الرياض، والدمام، وجدة، وعلى المتخصصين في المؤسسات الموفرة لتقنيات أمن نظم المعلومات في مدينة الرياض، كما يقتصر موضوع هذه الدراسة على جرائم نظم المعلومات ووسائل التحقيق فيها والمحدد بفترة تطبيقها لسنة (١٤٢٣هـ - ٢٠٠٢م).

٥-٥ مجتمع الدراسة

يقدر العدد الإجمالي لمجتمع الدراسة بحوالي (٤١٠) أفراد، ويتكون من ثلاثة شرائح وهي؛ شريحة المحققين في أقسام الشرطة المنتشرة في مدينة الرياض ومنسوبي الشؤون الفنية بوزارة الداخلية ويقدر عددهم الإجمالي بحوالي (١٣٢) فرداً. وشريحة العاملين في مجال نظم المعلومات والتي مؤسساتهم تستخدم نظم المعلومات لأداء نشاطها ويقدر عددهم الإجمالي بحوالي (١٨٢) فرداً. وشريحة المتخصصون بالمؤسسات الموفرة لتقنيات أمن نظم المعلومات ويقدر عددهم بحوالي (٩٦) فرداً.

٥-٦ عينة الدراسة

تم اختيار عينة عشوائية احتمالية طبقية Stratified Probability Random Sample لتقليل الاختلافات والتباينات بين مجموعات الدراسة وحتى لا يؤثر ذلك على النتائج (الضحيان، حسن، ١٤٢٣هـ: ٢٧١). وعليه فقد تم تحديد ثلاث طبقات كل طبقة تم اختيار عينة عشوائية بسيطة منها بواقع (٥٠٪) من المجتمع الأصلي، ومن ثم تمت إجراءات سحب العينة. وتضم الطبقة الأولى (٦٦) محققاً، والطبقة الثانية (٩١) عاملاً بمجال نظم المعلومات، والطبقة الثالثة (٤٨) متخصصاً في المؤسسات الموفرة لتقنيات أمن نظم المعلومات، ليبلغ مجموع العينة الكلي (٢٠٥) أفراد.

٥-٧ أداة الدراسة

٥-٧-١ بناء أداة الدراسة

بعد الإطلاع على أدبيات الدراسة والدراسات السابقة ذات الصلة بموضوع الدراسة، وبعد الزيارات الميدانية لمجتمع الدراسة للوقوف على واقع تلك الجرائم على أرض الميدان وفهم أساليبها وأدوات ارتكابها ووسائل التحقيق فيها وعلى مستوى أمن نظم المعلومات تم إعداد ثلاث إستبانات لكل عينة إستبانة، وذلك لجمع البيانات اللازمة للدراسة باعتبارها أنسب أدوات البحث العلمي الملائمة لتحديد استجابة العينة إزاء محاور الدراسة وللتعرف على آرائهم تجاه وسائل التحقيق في جرائم نظم المعلومات والتي من خلال الإجابة على تساؤلاتها يتم تحقيق أهداف الدراسة. وقد تبنى الباحث في إعداده لأداة الدراسة (الإستبان) الشكل المغلق (Closed Questionnaire) والذي يحدد الاستجابة المحتملة لكل سؤال. وقد تم استخدام عدة مقاييس منها، منها مقياس (Likert) للتدرج الخماسي لاستجابة عينة الدراسة إزاء عبارات الدراسة مثل (مهم جداً، مهم، مهم إلى حدٍ ما، غير مهم، غير مهم إطلاقاً). وملحق رقم (أ) يوضح أداة الدراسة (الإستبانة) بشكلها النهائي، والمتكونة من (١٩٤) فقرة، شاملة البيانات العامة، وستة محاور تفصيلية رئيسية، وهي كما يلي:

١. **البيانات العامة**

تتكون البيانات العامة من (٩) فقرات، ووجهت إلى العاملين بمجال نظم المعلومات فقط، وشملت على؛ الوظيفة الشخصية لأفراد العينة، وتم السؤال عنه بالفقرة (١). ونوع المؤسسة التي يعملون بها، وتم السؤال عنه بالفقرة (٢). وعدد أجهزة الحاسب الآلي في المؤسسة التي يعملون بها، وتم السؤال عنه بالفقرة (٣). ونسبة المصروفات على تقنية المعلومات إلى أجمالي ميزانية المؤسسة، وتم السؤال عنها بالفقرة (٤). وتوفر خدمة الإنترنت لموظفي المؤسسة، وتم السؤال عنه بالفقرة (٥). وأسلوب الدخول لشبكة الإنترنت في المؤسسة، وتم السؤال عنه بالفقرة (٦). ومدى وجود سياسة أمنية للتعامل مع الحاسبات الآلية والإنترنت بالمؤسسة، وتم السؤال عنه بالفقرة (٧). ومدى وجود قسم متخصص في أمن المعلومات، وتم السؤال عنه بالفقرة (٨). وعدد العاملين في قسم أمن المعلومات في المؤسسة، وتم السؤال عنه بالفقرة (٩).

٢. **المحور الأول/ مكونات السياسة**

يتكون هذا المحور من (١٢) فقرة، ووجهت إلى المحققين، والعاملين بمجال نظم المعلومات، والمتخصصين بالشركات الموفرة لتقنيات أمن نظم وشملت على؛ العناصر المتعلقة بمكوناتها، وتم السؤال عنها بالفقرات (من ١٠ إلى ١٤)، والعناصر الداخلة بمكوناتها، وتم السؤال عنها بالفقرات (من ١٥ إلى ٢٢).

٣. **المحور الثاني/ الإجراءات الإدارية والفنية لتحقيق أمن المعلومات**

يتكون هذا المحور من (٣٢) فقرة، ووجهت إلى عينة العاملين بمجال نظم المعلومات فقط وشمل على؛ مدى وعي العاملين بها، وتم السؤال عنه بالفقرة (٢٣). ومدى التوعية باتجاهها، وتم السؤال عنه بالفقرة (٢٤). ومدى إتباع إجراءات أمن المعلومات، وتم السؤال عنه بالفقرات (من ٢٥ إلى ٤٩).

٤. **المحور الثالث/ جرائم نظم المعلومات**

تكون هذا المحور من (٨١) فقرة، ووجه منها إلى العاملين بمجال النظم فقط عدد مرات حدوثها بالمؤسسات، وتم السؤال عنه بالفقرة (٥٠). وعدد الإنذارات بوجود جريمة عن طريق الإنترنت، وتم السؤال عنه بالفقرة (٥١). وتكلفتها، وتم السؤال عنها بالفقرة (٩٥). أما ما وجه إلى المحققين، والعاملين بمجال النظم أنماطها وحجم حدوثها بالمؤسسات، وتم السؤال عنها بالفقرات (من ٥٢ إلى ٦٥). ومدى الوعي بخطورتها، وتم السؤال عنه بالفقرة (٦٦). ومدى حدوثها بالمؤسسات، وتم السؤال عنه بالفقرات (من ٦٧ إلى ٦٩). ومستوى مكافحتها، وتم السؤال عنه بالفقرات (من ٧٠ إلى ٧٥). وحجم استخدام المنافذ الداخلية والخارجية للمؤسسات، وتم السؤال عنه بالفقرات (من ٩٦ إلى ١٠٣). وكيفية الحصول على الأدوات المستخدمة في ارتكابها من قبل مجرميها بالمملكة، وتم السؤال عنه بالفقرات (من ١٢٢ إلى ١٢٥). ودوافع ارتكابها، وتم السؤال عنه بالفقرات (من ١٢٦ إلى ١٣١). وأما ما وجه إلى العاملين بمجال النظم والمتخصصون بالمؤسسات الموفرة لتقنيات أمن نظم المعلومات أساليب ارتكابها، وتم السؤال عنه بالفقرات (من ٧٦ إلى ٩٤). الأدوات المستخدمة في ارتكابها، وتم السؤال عنها بالفقرات (من ١٠٤ إلى ١٢١).

٥. **المحور الرابع/ وسائل التحقيق في جرائم نظم المعلومات**

يتكون هذا المحور من (٣٤) فقرة، ووجه منها إلى المحققين، والعاملين بمجال نظم المعلومات الوسائل المستخدمة بضبطها، وتم السؤال عنها بالفقرات (١٣٢، ١٣٣، ١٣٨). والوسائل المستخدمة في تحديد مصدر وأدوات الهجوم على المؤسسات، وتم السؤال عنهما بالفقرتين (١٣٤، ١٣٥).الوسائل المستخدمة في تحديد شخصية مرتكبها وتم السؤال عنها بالفقرتين (١٣٦، ١٣٧). أما الوسائل المساعدة بضبط الجريمة، والتي تم السؤال عنها بالفقرات (من ١٤٥ إلى ١٥٦)، والوسائل المساعدة بالتحقيق، والتي تم السؤال عنها بالفقرات (من ١٥٧

إلى ١٦٦). فوجهت إلى المحققين، والعاملين بمجال نظم المعلومات، والمتخصصون بالمؤسسات الموفرة لتقنيات أمن نظم المعلومات.

٦. **المحور الخامس/ العوائق التي تحول دون استخدام تلك الوسائل**

يتكون هذا المحور من (٢٢) فقرة، ووجه منها إلى المحققين، والعاملين بمجال نظم المعلومات، والمتخصصون بالمؤسسات الموفرة لتقنيات أمن نظم المعلومات معوق عدم وجود تشريع واضح، وتم السؤال عنها بالفقرة (١٧٨). ومعوقات متعلقة بالجريمة، وتم السؤال عنها بالفقرتين (١٧٩،١٩٠). ومعوقات متعلقة بالجهات المتضررة من جرائم نظم المعلومات، وتم السؤال عنها بالفقرات (من ١٨٠ إلى ١٨٩) أما الفقرات من ١٣٩ إلى ١٤٤، والفقرتين ١٧٣، ١٧٤) وجهت إلى المحققين، والعاملين بمجال نظم المعلومات فقط. أما المعوقات المتعلقة بجهات التحقيق فوجهت إلى المحققين فقط وتم السؤال عنها بالفقرات (من ١٦٧ إلى ١٧٢، ومن ١٧٥ إلى ١٧٧).

٧. **المحور السادس/ الأدلة المثبتة في ارتكاب جرائم نظم المعلومات**

يتكون هذا المحور من (٤) فقرة، ووجهت إلى المحققين فقط وشملت على أنواع الأدلة المثبتة في ارتكاب جرائم نظم المعلومات، وتم السؤال عنها بالفقرات (من ١٩١ إلى ١٩٤).

٥-٧-٢ صدق الأداة

تم التحقق من الصدق الظاهري لأداة الدراسة في صورتها المبدئية وذلك بعرضها على نخبة من الأساتذة والخبراء من ذوي الاختصاص والاهتمام في مجال الحاسب الآلي وعلم الاجتماع وعلم النفس ومجال البحث العلمي والإحصاء بلغ عددهم (١٢) محكماً من أكاديمية نايف العربية للعلوم الأمنية، وجامعة الملك سعود، وجامعة الإمام محمد بن سعود الإسلامية، وكلية التقنية، والمركز الوطني للمعلومات بوزارة الداخلية، وإدارة التقنية البنكية بمؤسسة النقد العربي السعودي، ووحدة خدمات الإنترنت بمدينة الملك عبد العزيز للعلوم والتقنية. كما تم التأكد من الصدق الظاهري أيضاً

بتوزيعها على مجموعة مختارة من عينة الدراسة شملت؛ مدراء وأخصائيين أمن المعلومات بشركة الاتصالات وبعض القطاعات المصرفية، وشركة العلم لأمن المعلومات، وبعض الشركات الكبيرة، وقطاعات التحقيق بالأجهزة الأمنية والشركات الموفرة لأمن نظم المعلومات. وطلب الباحث من المحكمين، والعينة الاستطلاعية إبداء الرأي فيما يتعلق بمدى وضوح كل عبارة من عبارات أداة الدراسة ومدى مناسبتها لقياس ما وضعت من أجله ومدى ملائمة كل عبارة للمحور الذي تنتمي إلية، هذا بالإضافة إلى طلب اقتراح أي تعديلات على صياغة تلك العبارات أو الحذف منها أو الإضافة إليها.

كما تم التعرف على مدى فهم عينة الدراسة لأداة الدراسة وعلى ما يعيق إدراكهم تجاه تلك الأداة. وفي ضوء التوجيهات التي أبداها المحكمون قام الباحث بإجراء التعديلات التي اتفق عليها اثنان فأكثر من المحكمين كالعبارات غير الواضحة والتي رأى المحكمون إعادة صياغتها أو عبارات لم تكن موجودة ويجب ووضعها أو عبارات يجب حذفها. وبعد التأكد من الصدق الظاهري لأداة الدراسة قام الباحث بالتأكد من الصدق البنائي Construction Validity لأداة الدراسة، وذلك بتطبيقها على عيينة استطلاعية قوامها (٣٥) عاملاً في مجال نظم المعلومات وذلك لتحديد مدى التجانس الداخلي لأداة الدراسة بحساب معاملات الارتباط بين درجة كل عبارة من عبارات محاور الاستبانة ودرجة جميع عبارات محاور الإستبانة.

٣-٧-٥ ثبات الأداة

قام الباحث بالتأكد من ثبات Reliability أداة الدراسة بطريقة إعادة الاختبار، وذلك تطبيقها على عينة استطلاعية قوامها (٣٥) عاملاً في مجال نظم المعلومات. وتبين قيم معامل ألفا كرونباخ Alpha Cronbach أن ثبات الأداة كان (٠,٥٦٨٩).

٥-٨ إجراءات الدراسة

بعد الانتهاء من بناء أداة الدراسة (الإستبانة) ومن مراحل تطويرها والتأكد من صدق ثباتها، تم الحصول على خطاب تعريف من أكاديمية نايف العربية للعلوم الأمنية لتسهيل مهمة الباحث لدى الجهات ذات العلاقة، بالإضافة إلى أخذ الإذن من مدراء جهات مجتمع الدراسة للسماح بتوزيعها على عينة الدراسة في مؤسساتهم.

ومن ثم وزعت الإستبانات عشوائياً على أفراد عينة الدراسة، والبالغ عددهم (٢٠٥) أفراد، منهم (٦٦) محققاً واستجاب منهم (٣٦) يمثلون نسبة (٥٤,٦٪)، و(٩١) عاملاً بمجال نظم المعلومات استجاب منهم (٦٨) يمثلون نسبة (٧٤,٦٪)، و(٤٨) متخصصاً في المؤسسات الموفرة لتقنيات أمن نظم المعلومات استجاب منهم (٣٧) يمثلون نسبة (٧٧,١٪). ليصبح أجمالي الذين استجابوا من عينة الدراسة (١٤١) فرداً يمثلون (٦٨,٧٩٪) من مجموع عينة الدراسة، كما هو موضح في (جدول رقم ١، ملحق رقم ب) وتم توزيع الاستبانة على عينة الدراسة بالمناولة.

وحرصاً على سرية المعلومات في القطاعات المصرفية تم توزيع الإستبانة عن طريق إدارة التقنية البنكية بمؤسسة النقد العربي السعودي في مغّلف لا يحتوى على إسم الجهة والتي سوف تشارك بالدراسة لعدم الحاجة لمعرفة إسم القطاع المصرفي المشارك، وتم ذلك من خلال إحدى اجتماعات الإدارة بمدراء أمن نظم المعلومات في القطاعات المصرفية والذي يجمع حوالي (١٣) قطاعاً مصرفياً. وبشكل عام طلب الباحث من عموم المشاركين من خلال خطاب مرفق بالإستبانة التعاون معه بالإجابة على الإستبانة بدقة وعناية ودون تحفظ وأن المعلومات المستقاة ستكون موضع العناية والاهتمام والسرية التامة ولن تستخدم في أي غرض آخر سوى البحث العلمي فقط, وأثناء توزيع الاستبانات على عينة الدراسة تم الاتفاق على وقت التسليم والذي تم بالمناولة.

٥-٩ أساليب المعالجة الإحصائية

بعد ما تم جمع البيانات الخاصة بالدراسة قام الباحث بنفسه بتحليليها إحصائياً عن طريق إدخالها بالحاسب الآلي ومعالجة بياناتها ببرنامج (Statistical Package For Social Sciences) SPSS، وقد تم استخدام مجموعة من الأساليب الإحصائية، وذلك على النحو التالي:

١. النسب المئوية Percentages والتكرارات Frequencies وذلك لوصف خصائص العينة الدراسة والمؤسسات التي يعملون بها، بالإضافة لتحديد استجابة أفرادها تجاه عبارات المحاور الرئيسية التي تضمنتها أداة الدراسة.

٢. المتوسط الحسابي Mean وذلك لمعرفة مدى انخفاض وارتفاع استجابات عينة الدراسة تجاه عبارات المحاور الرئيسية التي تضمنتها أداة الدراسة. ويتم تحديد المتوسط الحسابي Mean بضرب تكرار الاستجابات كشكل (دائماً، غالباً، أحياناً، محدود، لا إطلاقاً) والمتوافقة مع التدرج الخماسي بالأعداد على الترتيب (من ٥ إلى ١) بحيث يعبر رقم (٥) عن أعلى قيمة، ورقم (١) أقل قيمة. أما النسبة المئوية للوسط الحسابي Mean فيتم تحديدها بضرب المتوسط الحسابي Mean بعدد (١٠٠) وقسمتها على عدد المستويات. ويتم الحصول على المتوسطات الحسابية على النحو التالي:

أ. متوسط (٤) إلى (٥) ويعبر عنه (عالي جداً، دائماً، موافق بشدة، مهم جداً، بدرجة كبيرة جداً) ويمثل النسبة من (٨٠,٠٪) إلى (١٠٠,٠٪) ويعني أنه عال جداً.

ب. متوسط من (٣,٢٥) إلى أقل من (٤) ويعبر عنه (عالي، غالباً، مهم، موافق، بدرجة كبيرة) ويمثل النسبة من (٦٥,٠٪) إلى أقل من (٨٠,٠٪) ويعني أنه عال.

ج. متوسط من (٢,٥٠) إلى أقل من (٣,٢٥) ويعبر عنه (متوسط، أحياناً، مهم إلى حدٍ ما، موافق إلى حدٍ ما، بدرجة متوسطة)، ويمثل النسبة من (٥٠,٠٪) إلى أقل من (٦٥,٠٪) ويعني أنه متوسط.

د. متوسط من (١,٧٥) إلى أقل من (٢,٥٠) ويعبر عنه (محدود، غير مهم، غير موافق، بدرجة محدودة) ويمثل النسبة من (٣٥,٠٪) إلى أقل من (٥٠,٠٪) ويعني أنه ضعيف.

هـ. متوسط أقل من (١,٧٥) ويعبر عنه (لا يوجد، لا يستخدم، لا يحدث، لا إطلاقاً، غير مهم إطلاقاً، غير موافق بشدة، لا أدري، لا يتبع إطلاقاً)، ويمثل نسبة أقل من (٣٥,٠٪) ويعني أنه ضعيف جداً.

٣. الانحراف المعياري Standard Deviation وهو الجذر التربيعي لمتوسط مربع انحرافات القيم عن متوسطها الحسابي كما هو أحد مقاييس التشتت Dispersion التي تستخدم للتعرف على مدى انحراف استجابات عينة الدراسة عن توسطها، أي مدى تشتتها أو تركزها عن الوسط (عودة، وملكاوي، ١٩٩٢م).

٤. معامل ارتباط سبيرمان Spearman Correlation Of Coefficient لتحديد مدى العلاقة بين متغيرات الدراسة، ويكون دال إحصائياً عند مستوى (٠,٠٥) فأقل أو (٠,٠١) فأقل (الضحيان، حسن، ١٤٢٣هـ: ١٦٦).

٥. معامل ارتباط كرونباخ ألفا Correlation Coefficient Cronbach Alpha لتحديد معامل ثبات أداة الدراسة. ومعامل الارتباط Correlation Of Coefficient لتحديد مدى الصدق البنائي والاتساق الداخلي لأداة الدراسة (الضحيان، حسن، ١٤٢٣هـ: ١٩٧)، والذي يكون مرتفعاً إذا كان (٠,٧٠) فأكثر (البداينة، ١٤٢٢هـ).

٦. تحليل التباين الأحادي Way ANOVA -One وذلك لمعرفة هل هناك فروق بين متغير إسمي Nominal Variables ومتغيرات رتبية Ordinal Variables، ويكون دال إحصائياً عند مستوى (٠,٠٥) فأقل (الضحيان، حسن، ١٤٢٣هـ: ١١٦).

٧. اختبار بيرسون كاي تربيع Person Chi-Square Tests لمعرفة هل هناك فروق جوهرية بين المتغيرات الاسمية Nominal Variables في هذه الدراسة، ويكون دال إحصائياً عند مستوى (٠,٠٥) فأقل (البداينة، ١٤٢٢هـ).

٨. اختبار شفية Scheffe حيث يستخدم لتحديد وجهة الفروق بين المتوسطات، ولصالح من يكون الفرق (الضحيان، حسن، ١٤٢٣هـ).

٩. تم استخدام برنامج SPSS في ترتيب الفقرات تنازلياً أما حسب حجمها، أو أهميتها، أو مدى الموافقة عليها أي كنظام مصفوفة ليسهل ملاحظتها وكذلك ترقيم تلك الجداول وعرضت كملحق بأخر هذه الرسالة والذي بدورة قد يحقق صحة عرض البيانات وعدم الوقوع بالخطاء.

٥-١٠ خلاصة الفصل الخامس

تم اعتماد المنهج المسحي بهذه الدراسة والتي تتكون عينتها من ثلاث طبقات رئيسية؛ وقد استجاب من الطبقة الأولى (المحققين) (٣٦) فرداً، ومن الطبقة الثانية (العاملين بمجال نظم المعلومات) (٦٨) فرداً، ومن الطبقة الثالثة (المتخصصين في المؤسسات الموفرة لتقنيات أمن نظم المعلومات) (٣٧) فرداً، ليصبح أجمالي الذين استجابوا من عينة الدراسة (١٤١) فرداً. كما تم إعداد إستبانة لجمع البيانات اللازمة للدراسة، والتي من خلال الإجابة على تساؤلاتها يتم تحقيق أهداف الدراسة، وتكونت من (١٩٤) فقرة. وبعد الانتهاء من توزيع الأستبانة وجمعها، قام الباحث بإدخال بيانات الدراسة ببرنامج SPSS وذلك للقيام بالتحليل الإحصائي، حيث تم استخدام مجموعة من الأساليب الإحصائية كالنسب المئوية Percentages والتكرارات Frequencies والمتوسط الحسابي Mean، والانحراف المعياري Standard Deviation، ومعامل ارتباط ألفا كرونباخ Cronbach Correlation Coefficient Alpha، واختبار التباين الأحادي (ف) One- Way ANOVA، واختبار بيرسون كاي تربيع Person Chi-Square Tests.

الفصل السادس/ نتائج الدراسة

٦-١ المقدمة

تحقيقاً لأهداف هذه الدراسة في تحديد وسائل التحقيق في مجال جرائم نظم المعلومات عن طريق الدراسة المسحية على المحققين بأقسام الشرطة في مدينة الرياض والشؤون الفنية بوزارة الداخلية، وعلى العاملين بمجال نظم المعلومات بالقطاع العام (مركز المعلومات الوطني بوزارة الداخلية، وإدارة التقنية البنكية بمؤسسة النقد العربي السعودي، ووحدة خدمات الإنترنت بمدينة الملك عبد العزيز للعلوم والتقنية)، والخاص (الشركات القابضة، الشركات المساهمة، والشركات الحكومية، والبنوك) والتي تستخدم نظم المعلومات لأداء نشاطها في مدن الرياض، والدمام، وجدة وعلى المتخصصين بالشركات الموفرة لتقنيات أمن نظم المعلومات في مدينة الرياض. حاول الباحث الكشف عن الجوانب المختلفة المحيطة بجريمة نظم المعلومات بتحديدها، ومعرفة دوافعها وإبراز أضرارها، وحصر الأساليب والأدوات المستخدمة من قبل مجرمي نظم المعلومات، وعن مكان توفر الأدوات المستخدمة في ارتكاب جرائم نظم من قبل مجرمي نظم المعلومات بالمملكة، والمنافذ المستخدمة من داخل المؤسسة أو من خارجها لارتكابها، وأدوات ضبط الجريمة والتحقيق فيها، وبيان العوائق التي تحول دون استخدام تلك الوسائل، وتحديد أنواع الأدلة المثبتة لارتكاب تلك الجرائم، وتحديد الإجراءات الأمنية سواء كانت فنية أو إدارية لتحقيق أمن نظم المعلومات، ومعرفة أسس صياغة إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات.

ولقد تم استهداف عينة عشوائية بلغ عدد أفرادها (١٤١) فرداً من مجتمع الدراسة والبالغ (٤١٠) أفراد، كما تم استخدام الإستبانة كأداة لجمع بيانات الدراسة، وقد حللت البيانات إحصائياً عن طريق إدخالها بالحاسب الآلي باستخدام مجموعة من أساليب الإحصاء المعروفة. وسيتناول الباحث في هذا الفصل خصائص العينة ونتائج الدراسة.

٢.٦ خصائص عينة الدراسة

اقتصرت خصائص عينة الدراسة على العاملين بمجال نظم المعلومات والمتكونة من (٦٨) فرداً. بسبب ما يهف إليه الباحث للحصول عن بيانات عن مؤسساتهم والتي تفيد في دراسة واقع الأمن، والجرائم، ووسائل التحقيق المتوفرة لدى تلك المؤسسات والتي لا توفر عند باقي العينة. ويظهر ملحق رقم (ب) من جدول رقم (٢) حتى جدول رقم (١٠) تلك الخصائص التي تم توزيعهم عليها، وهي على النحو التالي:

١. من ناحية نوع المؤسسة التي ينتمون إليها: يبلغ عدد الذين ينتمون إلى قطاع حكومي (١١) فرداً يمثلون نسبة (١٦,٢٪) من العينة، كما يبلغ عدد الذين ينتمون إلى قطاع مصرفي (١١) فرداً يمثلون نسبة (١٦,٢٪) من العينة، ويبلغ عدد الذين ينتمون إلى شركات متخصصة في مجال تقنية المعلومات (٣٤) فرداً يمثلون نسبته (٥٠,٠٪) من العينة، أما الذين ينتمون إلى شركات غير متخصصة في مجال تقنية المعلومات فيبلغ عددهم (١٢) فرداً يمثلون نسبة (١٧,٦٪). وهذا يشير إلى أن نصف عينة الدراسة من الشركات المتخصصة في مجال تقنية المعلومات.

٢. من ناحية تخصصاتهم: تتكون عينة الدراسة من عدد (١٤) إدارياً يمثلون نسبة (٢٠,٦٪)، وعدد (١١) مبرمجاً يمثلون نسبة (١٦,٢٪)، وعدد (٤) مديري النظام System admin يمثلون نسبة (٥,٩٪) وعدد (٤) مهندسي شبكات يمثلون نسبة (٥,٩٪)، وعدد (٧) محللي نظم يمثلون نسبة (١٠,٣٪)، وعدد (٣) مديري موقع Web Master يمثلون نسبة (٤,٤٪)، وعدد (٨) مدققاً Auditor يمثلون نسبة (١١,٨٪)، وعدد (٢) مديري قاعدة بيانات يمثلون نسبة (٢,٩٪)، وعدد (١٥) أخصائيي أمن معلومات يمثلون نسبة (٢٢,١٪). وهذا يشير إلى أن غالبية تخصصات عينة الدراسة من الإداريين، وأخصائيي أمن المعلومات، مع العلم أن غالبية التخصصات الأخرى هم من يعملون داخل أقسام الأمن، وهذا يعزى لاستهداف الباحث بدرجة الأولى الأقسام المتخصصة

بـأمن المعلومـات بالقطاعـات الكبيـرة والمسـؤولة عـن تـوفير الأمـن المعلومـاتي ليتحقـق الهـدف الرئيسي للدراسة بمعرفة وسائل التحقيق والتي قد لا يتوفر لدى الشركات الصغيرة.

٣. من ناحية عدد أجهزة الحاسبات التي تمتلكها مؤسساتهم: يبلغ عدد من يعمل في مؤسسات تملك أقل من (١٠٠) جهاز (٢٠) فرداً يمثلون نسبة (٢٩,٤٪)، وعدد (١٧) فرداً يمثلون نسبة (٢٥,٠٪) يعملون في مؤسسات تملك من (١٠٠) إلى (١٠٠٠) جهاز، وعدد (٣١) فرداً يمثلون نسبة (٤٥,٦٪) يعملون في مؤسسات تمتلك أكثر من (١٠٠٠) جهاز حاسب الآلي. وهذا يشير إلى أن حوالي نصف المؤسسات التي شملتها الدراسة تمتلك أكثر من (١٠٠٠) جهاز حاسب الآلي. ويستنتج مما سبق اعتماد جميع المؤسسات التي تناولتها الدراسة على نظم المعلومات لأداء نشاطها.

٤. من ناحية نسبة مصروفات المؤسسات على التقنية: يبلغ عدد الذين يعملون في مؤسسات تصرف نسبة أقل من (١٠٪) على تقنية المعلومات من إجمالي الميزانية (١٤) فرداً يمثلون نسبة (٢٠,٦٪)، وفي المؤسسات التي تصرف نسبة من (١٠٪) إلى أقل من (٣٠٪) يبلغ عددهم (١٢) فرداً يمثلون نسبة (١٧,٦٪)، وفي المؤسسات التي تصرف نسبة من (٣٠٪) إلى (٥٠٪) يبلغ عددهم (٢٩) فرداً يمثلون نسبة (٤٢,٦٪)، وفي المؤسسات التي تصرف نسبة أكثر من (٥٠٪) يبلغ عددهم (١٣) فرداً يمثلون نسبة (١٩,١٪). وهذا يشير إلى أن حوالي نصف المؤسسات تصرف على تقنية المعلومات نسبة من (٣٠٪) وأكثر من إجمالي الميزانية، وهذا يعزى إلى طبيعة المؤسسات التي شملتها الدراسة من القطاعات المصرفية والحكومية والشركات المتخصصة التي تصرف بشدة على التطبيقات التي ترقى بتقديم خدماتها والمحافظة على أمنها. كما يعزى أيضاً إلى أن غالبية الشركات المتخصصة تستثمر في الصرف على التقنية.

٥. من ناحية توفر الإنترنت للموظفين: الذين يعملون في مؤسسات توفر الإنترنت لجميع موظفيها يبلغ عددهم (٣٤) فرداً يمثلون نسبة (٥٠,٠٪) وعدد (٣٣) يمثلون نسبة (٤٨,٥٪) يعملون في

مؤسسات توفرها لبعض موظفيها فقط، بينما يبلغ عدد الذين يعملون في مؤسسات لا توفر الإنترنت لموظفيها إطلاقاً عدد (١) يمثل نسبة (١,٥٪). وهذا يشير إلى أن نسبة (٩٨,٥٪) من المؤسسات التي شملتها الدراسة توفر الإنترنت لموظفيها، كما يشير **أيضاً** على الاستخدام الكبير للإنترنت من قبل المؤسسات.

٦. من ناحية أسلوب الدخول للإنترنت: يبلغ عدد الذين ينتمون لمؤسسات ترتبط بالخطوط الهاتفية (dial up) عدد (٥) أفراد يمثلون نسبة (٧,٤٪)، وبالشبكة المحلية المربوطة بمزود الخدمة يبلغ عددهم (٥٩) فرداً يمثلون نسبة (٨٦,٨٪)، وعن طريق شبكة خاصة مستقلة عن شبكة العمل يبلغ عددهم (٣) أفراد يمثلون نسبة (٤,٤٪)، ويبلغ عدد الذين يعملون في مؤسسات لا ترتبط إطلاقاً بالإنترنت (١) يمثل نسبة (١,٥٪). وهذا يشير إلى أن غالبية المؤسسات التي شملتها الدراسة ترتبط بالشبكة المحلية المربوطة بمزود الخدمة.

٧. من ناحية وجود سياسة أمنية للتعامل مع الحاسب الآلي والإنترنت: يبلغ عدد الذين يعملون بمؤسسات يتوفر بها سياسات أمنية (٥٤) فرداً يمثلون نسبة (٧٩,٤٪) والذين يعملون بمؤسسات لا يوجد بها سياسات أمنية يبلغ عددهم (١٤) فرداً يمثلون نسبة (٢٠,٦٪). وهذا يشير إلى أن غالبية المؤسسات لديها سياسة أمنية، ويعزى هذا لكون الدراسة شملت القطاعات الكبيرة والتي لديها اهتمام كبير في مجال الأمن المعلوماتي ليتحقق الهدف الرئيسي للدراسة بمعرفة وسائل التحقيق والتي قد لا يتوفر لدى الشركات الصغيرة.

٨. من ناحية وجود قسم متخصص في أمن المعلومات: يبلغ عدد الذين يعملون بمؤسسات يوجد بها قسم متخصص في أمن المعلومات يبلغ عددهم (٥٠) فرداً يمثلون نسبة (٧٣,٥٪)، والذين يعملون بمؤسسات لا يوجد بها قسم متخصص يبلغ عددهم (١٨) فرداً يمثلون نسبة (٢٦,٥٪). وهذا يشير إلى أن غالبية المؤسسات لديها قسم متخصص في أمن المعلومات، ويعزى هذا لنفس السبب السابق والذي يتطلب من الباحث استهداف القطاعات الكبيرة والتي لديها اهتمام كبير في مجال

الأمن المعلوماتي ليتحقق الهدف الرئيسي للدراسة بمعرفة وسائل التحقيق والتي قد لا يتوفر لدى الشركات الصغيرة.

٩. من ناحية عدد العاملين في قسم الأمن: يبلغ عدد الذين ينتمون لمؤسسات عدد العاملين في قسم الأمن بها من (١) إلى (٥) يبلغ (١١) فرداً يمثلون نسبة (٢٠,٣٪)، وينتمي عدد (١٥) فرداً لمؤسسات عدد العاملين في قسم الأمن بها من (٦) إلى (١٠) يمثلون نسبة (٣٠,٨٪)، بينما ينتمي عدد (١٢) فرداً يمثلون نسبة (٢٤,٠٪) لمؤسسات عدد العاملين في قسم الأمن بها من (١١) إلى (٢٠)، وينتمي عدد (١٢) فرداً يمثلون نسبة (٢٤,٠٪) لمؤسسات عدد العاملين في قسم الأمن بها من (٢١) إلى (٥٠)، وعدد (١٨) فرداً ينتمون لمؤسسات لا يعمل بها متخصصين في مجال أمن المعلومات يمثلون نسبة (٢٠,٦٪). وهذا يشير إلى أن غالبية المؤسسات التي شملتها الدراسة يعمل بها متخصصون في أمن المعلومات.

٦-٣ نتائج الدراسة

لقد قامت هذه الدراسة بالإجابة على أسئلة الدراسة، وسيتم عرض نتائج الدراسة ووفقاً لتسلسل أسئلة الدراسة ابتداء بمكونات السياسة الأمنية الشاملة لحماية نظم المعلومات، ثم الإجراءات الفنية والإدارية لتحقيق أمن نظم المعلومات، وبعدها جرائم نظم المعلومات، ومن ثم وسائل التحقيق فيها، تليها العوائق التي تحول دون استخدامها وأخيراً أنواع الأدلة المثبتة لارتكابها، كما يبين ملحق رقم (جـ) جداول نتائج الدراسة من جدول رقم (١) حتى جدول رقم (٤٨).

٦-٣-١ مكونات السياسة الأمنية الشاملة لحماية نظم المعلومات

٦-٣-١-١ العناصر المتعلقة بمكوناتها

يظهر جدول رقم (١) استجابة عينة الدراسة والمكونة من (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) والبالغ عددهم (١٤١) فرداً إزاء

العناصر المتعلقة بمكونات السياسة الأمنية الشاملة لحماية نظم المعلومات، حيث جاءت النتائج على النحو التالي:

١. أكد ت إجابات أفراد العينة بدرجة قوية على عدم وجود سياسة أمنية واضحة لأمن نظم المعلومات بالمؤسسات، إذ بلغت نسبة الموافقين بشدة (٩٧,٢٪)، وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٩٦) ويمثل نسبة قدرها (٩٩,٢٪)، وهذا يشير إلى أن غالبية المؤسسات التي شملتها الدراسة لا تملك سياسة أمنية واضحة لأمن المعلومات برغم من أن ما نسبته (٧٩,٤٪) من عينة الدراسة يعملون بمؤسسات يتوفر بها سياسات أمنية، وهذا يدل على وجود السياسات الأمنية بغالبية المؤسسات دون أن تكون واضحة، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٢٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. يقتنع أفراد العينة بدرجة قوية بعدم اللزام الموظفين بالسياسة الأمنية ووضع عقوبات للمخالفين، إذ بلغت نسبة الموافقين بشدة (٩٣,٦٪)، وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٩٣) ويمثل نسبة قدرها (٩٨,٦٪)، وهذا يشير إلى أن غالبية المؤسسات التي شملتها الدراسة لا تلزم الموظفين بالسياسة الأمنية ولا تضع عقوبات للمخالفين، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٢٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٣. دلت إجابات أفراد العينة بدرجة قوية على عدم وجود سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية، إذ بلغت نسبة الموافقين بشدة (٩٠,١٪)، وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٩١) ويمثل نسبة قدرها (٩٨,٢٪)، وهذا يشير إلى أن غالبية المؤسسات التي شملتها الدراسة لا تملك سياسة أمنية معينة للتعامل مع من يرتكب الجرائم

المعلوماتية، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٢٩) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٤. أوضحت إجابات أفراد العينة بدرجة قوية نحو عدم إعلان السياسة الأمنية للموظفين بما يكفل تبليغها للعموم، إذ بلغت نسبة الموافقين بشدة (٨٥,٨٪)، وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٨٠) ويمثل نسبة قدرها (٩٦,٠٪)، وهذا يشير إلى أن غالبية المؤسسات التي شملتها الدراسة لا تعلن السياسة الأمنية للموظفين بما يكفل تبليغها للعموم، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٢٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٥. أشارت إجابات أفراد العينة بدرجة قوية نحو عدم تقيد الرؤساء بالسياسة الأمنية عند إعطاء التعليمات، إذ بلغت نسبة الموافقين بشدة (٤٦,١٪)، وقد جاء بالترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٤١) ويمثل نسبة قدرها (٨٨,٢٪)، وهذا يشير إلى أن غالبية العينة يرون عدم تقيد الرؤساء بالسياسة الأمنية عند إعطاء التعليمات، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٥٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

ويستنتج من المتوسط الحسابي Mean الأهمية القصوى لتوفر العناصر المتعلقة بالسياسة الأمنية وهي على الترتيب (حسب الأهمية)؛ وجود سياسة أمنية واضحة لأمن نظم المعلومات بالمؤسسات (٤,٩٦)، واللزام الموظفين بالسياسة الأمنية، ووضع عقوبات للمخالفين (٤,٩٣)، ووجود سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية (٤,٩١)، وإعلان السياسة الأمنية للموظفين بما يكفل تبليغها للعموم (٤,٨٠)، وتقيد الرؤساء بالسياسة الأمنية عند إعطاء التعليمات (٤,٤١). وهذا يحقق جزء من الهدف الأول من أهداف الدراسة.

٦-٣-١-٢ العناصر الداخلة بمكوناتها

تم أخذ آراء عينة الدراسة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) والبالغ عددهم (١٤١)، إزاء العناصر الداخلة بمكونات السياسة الأمنية الشاملة لحماية نظم المعلومات، والجداول على الترتيب من رقم (٢) إلى رقم (١٠) تظهر تلك الآراء على النحو التالي:

١. ذكر ما نسبته (٩٣,٧٪) من عينة الدراسة بأن عنصر الجانب البشري موجود من ضمن مكونات السياسة الأمنية بمؤسساتهم، مقابل ما نسبته (٦,٤٪) من عينة الدراسة ذكروا أنه ليس موجود وضرورياً، أما من ناحية وضوحه، فنسبة الذين ذكروا أنه واضح (٤٣,٣٪)، مقابل ما نسبته (٥٠,٤٪) ذكروا أنه غير واضح. وهذا يشير إلى وجود عنصر الجانب البشري من ضمن مكونات السياسة الأمنية لدى الغالبية العظمى من المؤسسات، كما يشير أنه غير واضح لدى نصف مؤسسات العينة.

٢. أكد ما نسبته (٩٥,٨٪) من عينة الدراسة بوجود عنصر الموقع المكاني لخدمات تقنية المعلوماتية من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٣,٥٪) أكدوا أنه ليس موجود وضرورياً، وما نسبته (٠,٧٪) أكدوا أنه ليس موجود وغير ضرورياً. أما من ناحية وضوحه، فنسبة الذين أكدوا أنه واضح (٨٠,٩٪)، مقابل ما نسبته (١٤,٩٪) أكدوا أنه غير واضح. وهذا يشير إلى وجود الموقع المكاني لخدمات تقنية المعلوماتية ووضوحه من ضمن مكونات السياسة الأمنية عند غالبية المؤسسات، ويعزى إلى نوعية المؤسسات التي شملتها الدراسة والتي تهتم بالجوانب الأمنية الأساسية والتقليدية، بحيث يعد هذا العنصر أسهل وأهم الإجراءات إتباعاً.

٣. أفاد ما نسبته (٧٧,٣٪) من عينة الدراسة بأن عنصر البرامج المطورة داخلياً موجود من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٢٠,٦٪) أفادوا أنه ليس موجود ولكن وجوده

ضروري، وما نسبته (٢,١٪) أفادوا أنه ليس موجود ووجوده غير ضروري، أما من ناحية وضوحه، فنسبة الذين أفادوا أنه واضح (٢٩,١٪)، مقابل ما نسبته (٤٨,٢٪) أفادوا أنه غير واضح. وهذا يشير إلى عدم وضوح عنصر البرامج المطورة داخلياً لدى حوالي نصف مؤسسات العينة برغم من وجوده في غالبية مكونات السياسة الأمنية لتلك المؤسسات.

٤. أشار ما نسبته (٥٨,٩٪) من عينة الدراسة بأن عنصر البرامج الجاهزة موجود من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٩,٩٪) أشاروا أنه ليس موجود وغير ضروري، وما نسبته (٢٠,٦٪) أشاروا أنه ليس موجود ووجوده ضرورياً، أما من ناحية وضوحه، فنسبة الذين أشاروا أنه واضح (٥٨,٩٪)، مقابل ما نسبته (٤٨,٢٪) أشاروا أنه غير واضح. وهذا يشير إلى وضوح عنصر البرامج المطورة داخلياً، ووجوده في غالبية المؤسسات من ضمن مكونات السياسة الأمنية.

٥. أوضح ما نسبته (٩٦,٤٪) من عينة الدراسة بأن عنصر استخدام الإنترنت موجود من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٢,٨٪) أوضحوا أنه ليس موجود وضرورياً، وما نسبته (٠,٧٪) أوضحوا أنه ليس موجود وغير ضرورياً، أما من ناحية وضوحه، فنسبة الذين أشاروا أنه واضح (٥٤,٦٪)، مقابل ما نسبته (٤١,٨٪) أوضحوا أنه غير واضح، وهذا يشير إلى وضوح استخدام الإنترنت عند أكثر من نصف مؤسسات العينة ووجوده في غالبية المؤسسات من ضمن مكونات السياسة الأمنية.

٦. كشف ما نسبته (٦٤,٥٪) من عينة الدراسة بأن عنصر التشارك في الخدمات موجود من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٠,٧٪) كشفوا أنه ليس موجود وغير ضرورياً، وما نسبته (٣٤,٨٪) كشفوا أنه ليس موجود وضرورياً، أما من ناحية وضوحه، فنسبة الذين كشفوا أنه واضح (٢٢,٧٪)، مقابل ما نسبته (٤١,٨٪) كشفوا أنه غير واضح. وهذا يشير إلى عدم

وضوح التشارك في الخدمات برغم من وجوده من ضمن مكونات السياسة الأمنية في غالبية المؤسسات.

٧. أكد ما نسبته (٥٨,٩٪) من عينة الدراسة بأن عنصر الاحترازات الشخصية موجود من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٠,٧٪) أكدوا أنه ليس موجود وغير ضرورياً، وما نسبته (٤٠,٤٪) أكدوا أنه ليس موجود وضرورياً، أما من ناحية وضوحه، فنسبة الذين أكدوا أنه واضح (٢٢,٧٪)، مقابل ما نسبته (٣٦,٢٪) أكدوا أنه غير واضح، وهذا يشير إلى عدم وضوح الاحترازات الشخصية برغم من وجودها في غالبية المؤسسات من ضمن مكونات سياستها الأمنية.

٨. أكد ما نسبته (٦٨,٨٪) من عينة الدراسة بأن عنصر الوثائق ووسائط الحفظ موجود من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٣١,٢٪) أكدوا أنه ليس موجود وضرورياً، أما من ناحية وضوحه، فنسبة الذين أكدوا أنه غير واضح (٤١,٨٪)، مقابل ما نسبته (٢٧,٠٪) أكدوا أنه وواضح، وهذا يشير إلى عدم وضوح البرامج المطورة داخلياً برغم من وجودها من ضمن مكونات السياسات الأمنية للمؤسسات.

٩. أشار ما نسبته (٤٩,٦٪) من عينة الدراسة بأن عنصر تحديد العلاقة بالمنافسين والشركاء موجود من ضمن مكونات السياسة الأمنية، مقابل ما نسبته (٢٦,٢٪) أشاروا أنه ليس موجود وضرورياً، وما نسبته (٢٤,١٪) أشاروا أنه ليس لديهم علم، أما من ناحية وضوحه، فنسبة الذين أشاروا أنه واضح (٢٤,١٪)، مقابل ما نسبته (٢٥,٥٪) أشاروا أنه موجود وغير واضح. وهذا يشير إلى عدم وجود عنصر تحديد العلاقة بالمنافسين والشركاء بالمؤسسات الموجود بها عند نصف مؤسسات عينة الدراسة، وعدم وضوحه عند حوالي نصف مؤسسات العينة من التي يوجد من ضمن مكونات سياستها الأمنية.

ويستنتج مما سبق أن أقل العناصر وضوحاً في مكونات السياسة الأمنية الشاملة بالمؤسسات على الترتيب الاحترازات الشخصية (٢٢,٧٪)، والتشارك في الخدمات (٢٢,٧٪)، والعلاقة بالمنافسين والشركاء (٢٤,١٪)، والوثائق ووسائط الحفظ (٢٧,٠٪)، والبرامج المطورة داخلياً (٢٩,١٪)، والجانب البشري (٤٣,٣٪). وهذا يجيب على جزء من السؤال الأول من أسئلة الدراسة (ما مدى وضوح تلك العناصر بالمؤسسات؟) كما يؤدى حصر تلك العناصر إلى الإجابة على جزء من السؤال الأول عن ما هي العناصر المكونة للسياسة الأمنية الشاملة لحماية نظم المعلومات وبالإجابة عليه يتحقق الهدف الأول من أهداف هذه الدراسة (وضع إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات).

٦-٣-٢ الإجراءات الفنية والإدارية لتحقيق أمن نظم المعلومات

تشمل هذه الفقرة على مدى وعي العاملين بالإجراءات الفنية والإدارية لتحقيق أمن نظم المعلومات، ومدى التوعية من قبل الإدارة تجاهه العاملين (بالقطاعين الحكومي، والمصرفي، والشركات المتخصصة وغير المتخصصة في مجال تقنية المعلومات)، كما تشمل على مدى إتباع تلك المؤسسات لإجراءات أمن المعلومات.

٦-٣-٢-١ مدى وعي العاملين بها والتوعية تجاهها

تم الوقوف على مدى وعي العاملين في نظم المعلومات (بالقطاعين الحكومي، والمصرفي، والشركات المتخصصة وغير المتخصصة في مجال تقنية المعلومات) والبالغ عددهم (٦٨)، والجدول رقم (١١) يوضح ذلك، كما تم الاطلاع على ما هو الأجراء المتبع تجاه توعيتهم بتلك الإجراءات الفنية والإدارية لتحقيق أمن نظم المعلومات، والجدول رقم (١٢) يوضح ذلك، ولقد كانت النتائج على النحو التالي:

١. يدرك أفراد العينة بدرجة قوية أهمية وجود إجراءات إدارية وفنية لأمن نظم المعلومات، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٩٣) ويمثل نسبة قدرها (٩٨,٦٪)، وقد بلغت نسبة ما يرون وجودها مهم جداً (٩٤,١٪)، ونسبة (٤,٤٪) يرونها مهمة، ونسبة (١,٥٪) يرونها مهمة إلى حدٍ ما. ويشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٣١)، إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. أبدا أفراد العينة أراءهم نحو كيفية التوعية في مجال أمن المعلومات بالمؤسسات، حيث بلغت نسبة الذين ذكروا أنها تتم عن طريق النشرات الداخلية (٤٧,٠٪)، وعن طريق الندوات والمحاضرات بلغت نسبتهم (١٨,١٪)، وعن طريق الاشتراكات بالمجلات والدوريات بلغت نسبتهم (٣٥,٣٪) والذين ذكروا أن التوعية تتم بها جميعاً بلغت نسبتهم (٢,٩٪) والذين ذكروا أن التوعية تتم بنشرات ودوريات فقط بلغت نسبتهم (٣٢,٤٪). ويستنتج مما سبق أن أقل الإجراءات التوعية أتباعاً التوعية بتلك العناصر السابقة مجتمعة، ثم الندوات والمحاضرات، ثم الاشتراكات بالمجلات والدوريات التي تعنى بأمن المعلومات.

٦-٣-٢-٢ مدى إتباع إجراءات أمن المعلومات

يوضح جدول رقم (١٣) استجابة العاملين في مجال نظم المعلومات (بالقطاعين الحكومي، والمصرفي، والشركات المتخصصة وغير المتخصصة في مجال تقنية المعلومات) والبالغ عددهم (٦٨) فرداً حول تقييمهم لمدى إتباع الإجراءات الأمنية بالمؤسسات، حيث يتضح إن أعلى الإجراءات الأمنية أتباعاً اختيار نوعية مناسبة من وسائل الحماية تلائم نوع التطبيق بمتوسط Mean يبلغ (٤,١٦)، وأقلها أتباعاً توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها بمتوسط Mean يبلغ (٢,٢٠). وقد جاءت النتائج على الترتيب (مرتبة حسب إتباعها من قبل العاملين بالمؤسسات):

١. أكد ما نسبته (٣٢,٤٪) من عينة الدراسة بأن اختيار نوعية مناسبة من وسائل الحماية تلائم نوع التطبيق يتبع دائماً، وما نسبته (٥٨,٨٪) أكدوا بأنه يتبع غالباً، مقابل ما نسبته (٣,٥٪) أكدوا بأن يتبع نادراً. وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,١٦) ويمثل نسبة قدرها (٨٣,٢٪)، مما يشير إلى أن المؤسسات دائماً تختار نوعية مناسبة من وسائل الحماية تلائم نوع التطبيق. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. كشف ما نسبته (٤,٤٪) من عينة الدراسة بأن توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم أنه يتبع دائماً، وما نسبته (٩٥,٦٪) كشفوا بأنه يتبع غالباً. وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٤) ويمثل نسبة قدرها (٨٠,٨٪)، وهذا يشير إلى أن المؤسسات دائماً تقوم بتوزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٢٠) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٣. أشار ما نسبته (١٠,٣٪) من عينة الدراسة بأن وضع الضوابط الأمنية لبناء وتشغيل البرامج التطبيقية يتبع دائماً, وما نسبته (٨٠,٩٪) أشاروا بأنه يتبع غالباً، مقابل ما نسبته (٥,٩٪) أشاروا بأنه يتبع نادراً. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٩٥) ويمثل نسبة قدرها (٧١,٨٪)، وهذا يشير إلى أن المؤسسات غالباً تضع الضوابط الأمنية لبناء وتشغيل البرامج التطبيقية، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٠) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٤. بين ما نسبته (١,٥٪) من عينة الدراسة بأن عدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين يتبع دائماً، وما نسبته (٩١,٢٪) بينوا بأنه يتبع غالباً، مقابل ما نسبته (١,٥٪) بينوا بأنه يتبع نادراً. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٩٢) ويمثل نسبة قدرها (٧٨,٤٪)، وهذا يشير إلى أن المؤسسات غالباً لا تسمح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٣٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٥. أوضح ما نسبته (٨,٨٪) من عينة الدراسة بأن اللزام العاملين بالنظم الإدارية المحددة يتبع دائماً، وما نسبته (٥٧,٤٪) أوضحوا بأنه يتبع غالباً، مقابل ما نسبته (١,٥٪) أوضحوا بأنه يتبع نادراً، وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٧٣) ويمثل نسبة قدرها (٧٤,٦٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم باللزام العاملين بالنظم الإدارية المحددة، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٣) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٦. أشار ما نسبته (٥,٩٪) من عينة الدراسة بأن الطلب ممن يلتحق حديثاً بالخدمة تزكية كشرط للتوظيف يتبع دائماً، وما نسبته (٦٦,٢٪) أشاروا بأنه يتبع غالباً، مقابل ما نسبته (٤,٤٪) أشاروا بأنه يتبع نادراً. وقد حاز على الترتيب السادس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٧٣) ويمثل نسبة قدرها (٧٤,٦٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم بالطلب ممن يلتحق حديثاً بالخدمة تزكية كشرط للتوظيف، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٣) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٧. أوضح ما نسبته (٣٢,٤٪) من عينة الدراسة بأن الإجراءات التي تكفل أمن النسخ الاحتياطي ووسائط الحفظ الخارجية تتبع دائماً، وما نسبته (٥,٩٪) أوضحوا بأنه يتبع غالباً. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٧١) ويمثل نسبة قدرها (٧٤,٢٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم بالإجراءات التي تكفل أمن النسخ الاحتياطي ووسائط الحفظ الخارجية. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٣) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٨. أدلى ما نسبته (٢٧,٩٪) من عينة الدراسة بأن الإجراءات الأمنية لصيانة الأجهزة تتبع دائماً، وما نسبته (١٠,٣٪) أدلوا بأنه يتبع غالباً. وقد حاز على الترتيب الثامن، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٦٦) ويمثل نسبة قدرها (٧٣,٢٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم بالإجراءات الأمنية لصيانة الأجهزة، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٩) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٩. أشار ما نسبته (٥٧,٤٪) من عينة الدراسة بأن ضوابط عمليات الإدخال والإخراج تتبع غالباً، مقابل ما نسبته (١٣,٢٪) أشاروا بأنه لا يتبع إطلاقاً. وقد حاز على الترتيب التاسع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٦١) ويمثل نسبة قدرها (٧٢,٢٪)، وهذا يشير إلى أن المؤسسات غالباً تضع ضوابط لعمليات الإدخال والإخراج، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٩) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

١٠. كشف ما نسبته (١٩,١٪) من عينة الدراسة بأن رصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم تتبع دائماً، وما نسبته (٣٨,٢٪) كشفوا بأنه يتبع غالباً، مقابل ما نسبته (١١,٨٪) كشفوا بأنه يتبع نادراً، وما نسبته (٧,٤٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب العاشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٥٠) ويمثل نسبة قدرها (٧٠,٠٪)، وهذا يشير إلى أن

المؤسسات غالباً تقوم برصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٥) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١١. يرى ما نسبته (٤٢,٦٪) من عينة الدراسة بأن الضوابط المنظمة لعمليات التشغيل تبع غالباً، مقابل ما نسبته (٤,٤٪) يرونه يتبع نادراً. وقد حاز على الترتيب الحادي عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٣٨) ويمثل نسبة قدرها (٦٧,٦٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم بوضع الضوابط المنظمة لعمليات التشغيل، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٦) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٢. أشار ما نسبته (٢٣,٥٪) من عينة الدراسة بأن تحديث برامج الحماية باستمرار يتبع دائماً، وما نسبته (٤٤,١٪) أشاروا بأنه يتبع غالباً، مقابل ما نسبته (٨,٨٪) أشاروا بأنه يتبع نادراً، وما نسبته (١٧,٦٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب الثاني عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٤٧) ويمثل نسبة قدرها (٦٩,٤٪)، وهذا يشير إلى أن المؤسسات غالباً تحدث برامج الحماية باستمرار، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٤٠) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٣. أوضح ما نسبته (١٧,٦٪) من عينة الدراسة بأن استخدام وسائل حماية تساعد في تتبع المجرمين يتبع دائماً، وما نسبته (٢٧,٩٪) أوضحوا بأنه يتبع غالباً، مقابل ما نسبته (٥,٩٪) أوضحوا بأنه يتبع نادراً، وما نسبته (١٠,٣٪) أوضحوا بأنه لا يتبع إطلاقاً. وقد حاز على الترتيب الثالث عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٣٦) ويمثل نسبة قدرها (٦٧,٢٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم باستخدام وسائل حماية تساعد في تتبع

المجرمين، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٦) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٤. أفاد ما نسبته (٢٧,٩٪) من عينة الدراسة بأن التدريب الدوري على أمن المعلومات يتبع دائماً، وما نسبته (٢٣,٥٪) أفادوا بأنه يتبع غالباً، مقابل ما نسبته (٢,٩٪) أفادوا بأنه يتبع نادراً، وما نسبته (٢٠,٦٪) أفادوا بأنه لا يتبع إطلاقاً. وقد حاز على الترتيب الرابع عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٣٥) ويمثل نسبة قدرها (٦٧,٠٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم بالتدريب الدوري على أمن المعلومات، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٤٥) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٥. أكد ما نسبته (٧٩,٨٪) من عينة الدراسة بأن ضوابط إدارة الشبكات وخطوط الاتصال تتبع دائماً، وما نسبته (٩,٦٪) أكدوا بأنه يتبع غالباً، مقابل ما نسبته (٣,٨٪) أكدوا بأنه يتبع نادراً، وما نسبته (٩,٦٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب الخامس عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٣٠) ويمثل نسبة قدرها (٦٦,٠٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم بإتباع ضوابط إدارة الشبكات وخطوط الاتصال تلائم نوع التطبيق، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٤) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

١٦. أشار ما نسبته (٢٦,٥٪) من عينة الدراسة بأن استخدام التقنية للدخول على الأنظمة يتبع دائماً، وما نسبته (٣٨,٢٪) أشاروا بأنه يتبع غالباً، مقابل ما نسبته (٢,٩٪) أشاروا بأنه يتبع نادراً، وما نسبته (٢٧,٩٪) أشاروا بأنه لا يتبع إطلاقاً. وقد حاز على الترتيب السادس عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٣٢) ويمثل نسبة قدرها (٦٦,٤٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم باستخدام التقنية للدخول على الأنظمة، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٥٩) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٧. كشف ما نسبته (٥٧,٤٪) من عينة الدراسة بأن وضع ضوابط مبرمجي قواعد البيانات ومدرائها يتبع غالباً، مقابل ما نسبته (١٣,٢٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب السابع عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٣٠) ويمثل نسبة قدرها (٦٦,٠٪)، وهذا يشير إلى أن المؤسسات غالباً تقوم بوضع ضوابط لمبرمجي قواعد البيانات ومدرائها. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٠١) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٨. بينت إجابات عينة الدراسة بأن ما نسبته (٧٩,٨٪) منهم يرون أن تحديث النسخ الاحتياطي المركزي يتبع دائماً، وما نسبته (٩,٦٪) يرونه يتبع غالباً، مقابل ما نسبته (٣,٨٪) يرونه يتبع نادراً، وما نسبته (٩,٦٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب الثامن عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,١٩) ويمثل نسبة قدرها (٦٣,٨٪)، وهذا يشير إلى أن المؤسسات أحياناً تقوم بتحديث النسخ الاحتياطي المركزي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٣٩) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٩. أشارت إجابات عينة الدراسة بأن ما نسبته (٨,٨٪) منهم يرون أن تشكيل فريق طوارئ للتعامل مع الجريمة يتبع دائماً، وما نسبته (٣٨,٢٪) يرونه يتبع غالباً، مقابل ما نسبته (٣٣,٨٪) يرونه يتبع نادراً، و٥ (٧,٤٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب التاسع عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٠٧) ويمثل نسبة قدرها (٦١,٤٪)، وهذا يشير إلى أن المؤسسات أحياناً تقوم بتشكيل فريق طوارئ للتعامل مع الجريمة، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٧) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٢٠. أفاد ما نسبته (٢٦,٥٪) من عينة الدراسة بأن التقدم بشكوى حول جرائم نظم المعلومات يتبع غالباً، مقابل ما نسبته (٣٠,٩٪) أفادوا بأنه يتبع نادراً. وقد حاز على الترتيب العشرون، حيث

بلغت قيمة المتوسط الحسابي Mean (٢,٩٥) ويمثل نسبة قدرها (٥٩,٠٪)، وهذا يشير إلى أن المؤسسات أحياناً تتقدم بشكوى حول جرائم نظم المعلومات، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢١. يرى ما نسبته (٣٥,٣٪) من عينة الدراسة بأن تحديد مدة صلاحية كلمات المرور وتغييرها يتبع غالباً، مقابل ما نسبته (٥٤,٤٪) يرونه يتبع نادراً، وما نسبته (٢,٩٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب الواحد والعشرون، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٧٥) ويمثل نسبة قدرها (٥٥,٠٪)، وهذا يشير إلى أن المؤسسات أحياناً تقوم بتحديد مدة صلاحية كلمات المرور وتغييرها، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢٢. يرى ما نسبته (٥,٩٪) من عينة الدراسة بأن ربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات يتبع دائماً، وما نسبته (٢٦,٥٪) يرونه يتبع غالباً، مقابل ما نسبته (١٩,١٪) يرونه يتبع نادراً، وما نسبته (٢٦,٥٪) يرونه لا يتبع إطلاقاً. وقد حاز على الترتيب الثاني والعشرون، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٦٦) ويمثل نسبة قدرها (٥٣,٢٪)، وهذا يشير إلى أن المؤسسات أحياناً تقوم بربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٩) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٢٣. أفاد ما نسبته (١٣,٢٪) من عينة الدراسة بأن التأكد من مزامنة ساعات الأجهزة باستمرار يتبع دائماً، وما نسبته (٥,٩٪) أفادوا بأنه يتبع غالباً، مقابل ما نسبته (٣٥,٣٪) أفادوا بأنه يتبع نادراً، وما نسبته (٢٦,٥٪) أفادوا بأنه لا يتبع إطلاقاً. وقد حاز على الترتيب الثالث والعشرون، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٤٤) ويمثل نسبة قدرها (٤٨,٨٪)، وهذا يشير إلى أن

المؤسسات من النادر أن تقوم بالتأكد من مزامنة ساعات الأجهزة باستمرار، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٣٠) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٢٤. أشار ما نسبته (١١,٨٪) من عينة الدراسة بأن منح الحوافز للالتزام بالإجراءات الأمنية يتبع دائماً، مقابل ما نسبته (٥١,٥٪) أشاروا بأنه يتبع نادراً، وما نسبته (٢٣,٥٪) أشاروا بأنه لا يتبع إطلاقاً. وقد حاز على الترتيب الرابع والعشرون، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٢٥) ويمثل نسبة قدرها (٤٥,٠٪)، وهذا يشير إلى أن المؤسسات من النادر أن تقوم بمنح الحوافز للالتزام بالإجراءات الأمنية، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٧) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٢٥. ذكر ما نسبته (٥,٩٪) من عينة الدراسة بأن توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها يتبع غالباً، مقابل ما نسبته (٤٢,٦٪) ذكروا بأنه لا يتبع إطلاقاً. وقد حاز على الترتيب الخامس والعشرون والأخير، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٢٠) ويمثل نسبة قدرها (٤٤,٠٪)، وهذا يشير إلى أن المؤسسات من النادر أن تقوم بتوفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٠٧) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

ويستنتج من قيمة المتوسط الحسابي Mean أن أقل الإجراءات أتباعاً (على الترتيب) توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها (٢,٢٠)، ومنح الحوافز للالتزام بالإجراءات الأمنية (٢,٢٥)، والتأكد من مزامنة ساعات الأجهزة باستمرار (٢,٤٤)، وربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات (٢,٦٦)، وتحديد مدة صلاحية كلمات

المرور وتغييرها (٢,٧٥)، والتقدم بشكوى حول جرائم نظم المعلومات (٢,٩٥)، وتحديث النسخ الاحتياطي المركزي (٣,٠٧). وهذا يدل على أن هناك قصور أمني بإتباع تلك الإجراءات.

كما يستنتج من الانحراف المعياري Std.Deviation عدم تقارب وتركز إجابات العينة وتشتتها عند الإجراءات التالية (مرتبة تنازلياً) استخدام التقنية للدخول على الأنظمة (بصمة الإصبع، بصمة العين، البطاقات الممغنطة) (١,٥٩)، التدريب الدوري على أمن المعلومات (١,٤٥)، تحديث برامج الحماية باستمرار (١,٤٠)، تحديث النسخ الاحتياطي المركزي (١,٣٩)، التأكد من مزامنة ساعات الأجهزة باستمرار (١,٣٠)، ربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات (١,٢٩)، الضوابط المنظمة لعمليات التشغيل (١,٢٦)، منح الحوافز للالتزام بالإجراءات الأمنية (١,١٧)، تشكيل فريق طوارئ للتعامل مع الجريمة (١,١٧)، استخدام وسائل حماية تساعد في تتبع المجرمين (١,١٦)، رصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم (١,١٥)، توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها (١,٠٧)، ضوابط مبرمجي قواعد البيانات ومدرائها (١,٠١). وهذا يدل على اختلاف الإجراءات الأمنية المتبعة بالمؤسسات، ويعزى إلى نوع المؤسسات المشمولة بهذه الدراسة إذ يعتمد مستوى الأمن لديها على درجة أهمية معلوماتها والنشاط الذي تمارسه تلك المؤسسات.

٦-٣-٣ جرائم نظم المعلومات

شملت هذه الفقرة عرض استجابة عينة الدراسة نحو أنواع جرائم نظم المعلومات وحجم حدوثها بالمؤسسات، ومدى الوعي بخطورتها، ومدى حدوثها بالمؤسسات، والأساليب المستخدمة في ارتكابها، ومنافذ المؤسسة المستخدمة في ارتكابها، والأدوات المستخدمة من قبل مجرميها، وحجم الحصول علي أدوات ارتكابها بالمملكة، ومستوى مكافحتها، ودوافعها، وتكلفتها.

٦-٣-٣-١ أنماطها وحجم حدوثها بالمؤسسات

يوضح جدول رقم (١٤) استجابة عينة الدراسة (المحققين بالأجهزة الأمنية والعاملين في مجال نظم المعلومات) والبالغ عددهم (١٠٤) أفراد إزاء أنواع وحجم حدوث جرائم نظم المعلومات بالمؤسسات، حيث يتضح إن أعلى الجرائم حدوثاً إرسال وزراعة الفيروسات، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٦)، وأقلها حدوثاً إغراق البريد الإلكتروني، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٧٥). وقد جاءت النتائج على الترتيب (مرتبة حسب حجم حدوثها بالمؤسسات):

١. أوضح ما نسبته (٧٩,٨٪) من عينة الدراسة بأن حجم حدوث إرسال وزراعة الفيروسات عالي، مقابل ما نسبته (٣,٨٪) أوضحوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (٩,٦٪) أوضحوا بأنها لا تحدث، وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٦) ويمثل نسبة قدرها (٨١,٢٪)، وهذا يشير إلى أن حجم حدوث إرسال وزراعة الفيروسات بالمؤسسات عالي جداً. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٦) إلى عدم تركز الإجابات وتشتتها.

٢. أفاد ما نسبته (٥٦,٧٪) من عينة الدراسة بأن حجم حدوث نسخ البرامج والاستخدام غير المصرح به عالي، مقابل (١٩,٢٪) أفادوا بأن حجم حدوث هذه الجريمة محدود، وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٩) ويمثل نسبة قدرها (٧٧,٨٪)، وهذا يشير إلى أن حجم حدوث نسخ البرامج والاستخدام غير المصرح به بالمؤسسات عالي. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٤) إلى عدم تركز الإجابات وتشتتها.

٣. أفاد ما نسبته (٦٦,٣٪) من عينة الدراسة بأن حجم حدوث التلاعب بإدخال البيانات عالي، مقابل ما نسبته (٥,٨٪) أفادوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (٤,٨٪) أفادوا بأن تلك الجريمة لا تحدث، وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean

(٣,٨٨) ويمثل نسبة قدرها (٧٧,٦٪)، وهذا يشير إلى أن حجم التلاعب بإدخال البيانات بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٢) إلى عدم تركز الإجابات وتشتتها.

٤. أشار ما نسبته (٧٠,٢٪) من عينة الدراسة بأن حجم حدوث تغيير البرامج والإعدادات عالي, مقابل ما نسبته (٨,٧٪) أشاروا بأن حجم حدوث هذه الجريمة محدود، وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٦) ويمثل نسبة قدرها (٧٧,٢٪)، وهذا يشير إلى أن حجم تغيير البرامج والإعدادات بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٩) إلى تركز الإجابات وعدم تشتتها.

٥. أكد ما نسبته (٦,٧٪) من عينة الدراسة بأن حجم إرسال أحصنة طروادة عالي، مقابل ما نسبته (٨,٧٪) أكدوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (١,٩٪) أكدوا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٣) ويمثل نسبة قدرها (٧٦,٦٪)، وهذا يشير إلى أن حجم إرسال أحصنة طروادة بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٦) إلى تركز الإجابات وعدم تشتتها.

٦. كشف ما نسبته (٤٧,١٪) من عينة الدراسة بأن حجم الاستيلاء على ما سوى المعلومات عالي، مقابل ما نسبته (٥,٨٪) كشفوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (٤,٨٪) كشفوا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب السادس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٤٠) ويمثل نسبة قدرها (٦٨,٠٪)، وهذا يشير إلى أن حجم الاستيلاء على ما سوى المعلومات بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٨) إلى تركز الإجابات وعدم تشتتها.

٧. أشار ما نسبته (٥١,٠٪) من عينة الدراسة بأن حجم حدوث تغيير البيانات بعد إدخالها عالي، مقابل ما نسبته (٤,٨٪) أشاروا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (١٤,٤٪) أشاروا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٣٢) ويمثل نسبة قدرها (٦٦,٤٪)، وهذا يشير إلى أن حجم تغيير البيانات بعد إدخالها عالي، كما يشير الانحراف المعياري والبالغ قدرة (١,٢٣) إلى تركز الإجابات وعدم تشتتها.

٨. أفاد ما نسبته (٣٦,٥٪) من عينة الدراسة بأن حجم حدوث تدمير الملفات وقواعد البيانات عالي، مقابل ما نسبته (١٢,٥٪) أفادوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (١,٩٪) أفادوا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب الثامن، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٢٦) ويمثل نسبة قدرها (٦٥,٢٪)، وهذا يشير إلى أن حجم تدمير الملفات وقواعد البيانات بالمؤسسات عالي، كما يشير الانحراف المعياري والبالغ قدرة Std.Deviation (٠,٧٨) إلى تركز الإجابات وعدم تشتتها.

٩. أوضح ما نسبته (٥٢,٩٪) من عينة الدراسة بأن حجم حدوث اختراقات البريد الإلكتروني عالي، مقابل ما نسبته (٦,٧٪) أوضحوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (١٢,٥٪) أوضحوا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب التاسع، وبلغت قيمة المتوسط الحسابي Mean (٣,٢٤) ويمثل نسبة قدرها (٦٤,٨٪)، وهذا يشير إلى أن حجم اختراقات البريد الإلكتروني بالمؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٠٧) إلى عدم تركز الإجابات وتشتتها.

١٠. أشار ما نسبته (٥٠,٠٪) من عينة الدراسة بأن حجم حدوث نسخ البيانات لاستفادة منها عالي، مقابل ما نسبته (١٤,٤٪) أشاروا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (١٤,٤٪) أشاروا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب العاشر، و بلغت قيمة المتوسط الحسابي

Mean (٣,١٣) ويمثل نسبة قدرها (٦٢,٦٪)، وهذا يشير إلى أن حجم نسخ البيانات لاستفادة منها بالمؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٠٧) إلى عدم تركز الإجابات وتشتتها.

١١. أفاد ما نسبته (٢٠,٢٪) من عينة الدراسة بأن حجم حدوث اعتراض الرسائل والتنصت عالي، مقابل ما نسبته (٣,٨٪) أفادوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (٣,٨٪) أفادوا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب الحادي عشر، وبلغت قيمة المتوسط الحسابي Mean (٣,٠٩) ويمثل نسبة قدرها (٦١,٨٪)، وهذا يشير إلى أن حجم اعتراض الرسائل والتنصت بالمؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٢) إلى تركز الإجابات وعدم تشتتها.

١٢. أشار ما نسبته (٣٢,٧٪) من عينة الدراسة بأن حجم حدوث التنصت والسرقة البيانات عالي، مقابل ما نسبته (٤,٨٪) أشاروا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (١٤,٤٪) أشاروا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب الثاني عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٩٩) ويمثل نسبة قدرها (٥٩,٨٪)، وهذا يشير إلى أن حجم التنصت والسرقة البيانات متوسط. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٦) إلى تركز الإجابات وعدم تشتتها.

١٣. أفادا ما نسبته (٣٢,٩٪) من عينة الدراسة بأن حجم حدوث تعطيل المواقع والبرامج والأجهزة عالي، مقابل ما نسبته (٨,٧٪) أفادوا بأن حجم حدوث هذه الجريمة محدود، وما نسبته (٢٠,٢٪) أفادوا بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب الثالث عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٨٧) ويمثل نسبة قدرها (٥٧,٤٪)، وهذا يشير إلى أن حجم تعطيل المواقع والبرامج والأجهزة بالمؤسسات متوسط. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٣) إلى عدم تركز الإجابات وتشتتها.

١٤. يرى ما نسبته (١٥,٤٪) من عينة الدراسة بأن حجم إغراق البريد الإلكتروني عالي، مقابل ما نسبته (١٢,٥٪) يرون بأن حجم حدوث هذه الجريمة محدود، وما نسبته (٢٠,٢٪) يرون بأن تلك الجريمة لا تحدث. وقد حاز على الترتيب الرابع عشر والأخير، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٧٥) ويمثل نسبة قدرها (٥٥,٠٪)، وهذا يشير إلى أن حجم إغراق البريد الإلكتروني بالمؤسسات متوسط. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٩) إلى عدم تركز الإجابات وتشتتها.

ويستنتج مما سبق أن هناك جرائم حجم حدوثها بالمؤسسات عالي وهي على الترتيب؛ إرسال وزراعة الفيروسات (٤,٠٦)، ونسخ البرامج والاستخدام غير المصرح به (٣,٨٩)، والتلاعب بإدخال البيانات (٣,٨٨)، وتغيير البرامج والإعدادات (٣,٨٦)، وإرسال أحصنة طروادة (٣,٨٣)، والاستيلاء على ما سوى المعلومات (٣,٤٠)، وتغيير البيانات بعد إدخالها (٣,٣٢)، وتدمير الملفات وقواعد البيانات (٣,٢٦).

يتفق هذا مع ما توصلت إلية دراسة (Rapalus) والتي أفادت أن نسبة (٩٠٪) من المجيبين (وغالبيتهم من المؤسسات الكبرى والهيئات الحكومية) اكتشفوا مخالفات أمنية لحاسباتهم الآلية، وأن (٩١٪) اكتشفوا إساءة استخدام موظفين لديهم لشبكة الإنترنت مثل قرصنة البرمجيات وطباعة محتوياتها أو استخدام غير لائق لنظم البريد الإلكتروني، وأن (١٣٪) أبلغوا عن سرقة معلومات أو بيانات تتعلق بمعاملات تجارية، و(٤٠٪) اكتشفوا أن النظام المعلوماتي لديهم قد تم اختراقه من الخارج, وأن (٩٤٪) اكتشفوا فيروسات حاسب آلي، و(٩٠٪) ابلغوا عن عمليات تخريب، و(٨٪) ابلغوا عن حالات احتيال أو تزوير مالي (Rapalus, ٢٠٠٢). كما تتفق مع دراسة (الهاجري) حول أنواع الجرائم التي تستهدف المعلومات ولأجهزة ولكنها تختلف عنها بأن دراسته لم تحدد حجم تلك الجرائم بالمؤسسات.

٦-٣-٣-٢ مدى الوعي بخطورتها

لأجل معرفة وعي وأدراك عينة الدراسة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات) بخطورة جرائم نظم المعلومات تم أخذ آراءهم إزاء خطورة جرائم نظم المعلومات، والجدول رقم (١٥) يوضح أن ما نسبته (٩٠,٤٪) من عينة الدراسة يرون خطورة جرائم نظم المعلومات عالية، مقابل ما نسبته (١,٩٪) بأن خطورتها محدودة، وما نسبته (١,٠٪) يرونها ليست خطيرة. وقد بلغت قيمة المتوسط الحسابي Mean (٤,٥٨) ويمثل نسبة قدرها (٩١,٦٪)، وهذا يشير إلى أن عينة الدراسة تدرك بدرجة قوية جداً خطورة جرائم نظم المعلومات، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها. وهذا يتفق مع دراسة (الشهري، ١٤٢٢هـ). حيث أفاد بأن ما نسبته (٧٩,١٪) من العاملين بالأجهزة الأمنية بوعيهم وإدراكهم ومعرفتهم بجرائم نظم المعلومات وأنماطها. ويعزي الباحث هذا إلى انتشار التقنية في المجتمع وسهولة التعامل معها.

٦-٣-٣-٣ مدى حدوثها بالمؤسسات

لأجل معرفة مدى حدوثها بالمؤسسات أخذ آراءهم حول معدلها بعد ظهور الإنترنت، وحجمها مقارنة بحجم الجرائم الأخرى في المؤسسات، ومدى الإعلان عنها في المؤسسات، وجدول رقم (١٥) يوضح ذلك، ولمعرفة مدى حدوثها أيضاً تم أخذ آراء عينة الدراسة (العاملين في مجال نظم المعلومات فقط) إزاء عدد مرات حدوث جرائم نظم المعلومات بالمؤسسات وجدول رقم (١٦) يوضح ذلك، وأيضاً تم أخذ آراء عينة الدراسة (العاملين في مجال نظم المعلومات فقط) حيال عدد الإنذارات بوجود جريمة ترتكب عن طريق الإنترنت وذلك لمعرفة مدى حدوثها وجدول رقم (١٧) يوضح ذلك، أما النتائج بالتفصيل على النحو التالي:

١. أفاد ما نسبته (٧٧,٩٪) من عينة الدراسة بأن معدل جرائم نظم المعلومات بعد ظهور الإنترنت عالي. وقد بلغت قيمة المتوسط الحسابي Mean (٤,٤٨) ويمثل نسبة قدرها (٨٩,٦٪)، وهذا

يشير إلى أن معدل جرائم نظم المعلومات بعد ظهور الإنترنت عالي جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٤٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. أشار ما نسبته (٦٩,٣٪) من عينة الدراسة بأن حجم جرائم نظم المعلومات مقارنة بحجم الجرائم الأخرى في المؤسسات عالي، مقابل ما نسبته (٢٨,٨٪) أشاروا بأن حجمها محدود، وما نسبته (١,٠٪) أشاروا بأنها لا تحدث. وقد بلغت قيمة المتوسط الحسابي Mean (٣,٦٢) ويمثل نسبة قدرها (٧٢,٤٪)، وهذا يشير إلى أن حجم جرائم نظم المعلومات مقارنة بحجم الجرائم الأخرى في المؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٦) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٣. أفاد ما نسبته (٦٣,٤٪) من عينة الدراسة بأن الإعلان عن الجرائم في المؤسسات عالي، مقابل ما نسبته (٣٤,٦٪) أفادوا بأنه محدود، وما نسبته (٩,٦٪) أفادوا بأنه لا يعلن عنها، وقد بلغت قيمة المتوسط الحسابي Mean (٢,٧٥) ويمثل نسبة قدرها (٥٥,٠٪)، وهذا يشير إلى أن حجم الإعلان عن الجرائم في المؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٤. أفاد ما نسبته (٢٣,٥٪) من عينة الدراسة بأن جرائم نظم المعلومات تحدث بشكل يومي على الأقل بمؤسساتهم، كما أفاد ما نسبته (٤٧,١٪) بأنها تحدث بشكل غير منتظم على الأقل. وهذا يشير إلى أن عدد مرات حدوث جرائم نظم المعلومات بالمؤسسات مرتفع.

٥. بلغت نسبة الذين لم يستجيبوا من عينة العاملين في مجال نظم المعلومات حيال عدد الإنذارات عن وجود جريمة عن طريق الإنترنت (٣٥,٣٪)، وذلك بسبب ما أبدوه عينة الدراسة من عدم توفر أجهزة إنذار Alarms تعطي عدد الجرائم التي تحدث بمؤسساتهم على غرار باقي العينة، كما

أبدا بعضهم أنه لا يعمل علي تلك الأجهزة أو ليست موجودة بقسمه. أما ما استجاب منهم بلغت نسبتهم (٦٤,٧٪)، حيث أشار ما نسبته (٣٤,١٪) منهم بأن مؤسساتهم تتعرض إلى إنذارات عن طريق الإنترنت تصل من (١٠) إلى أقل من (١٠٠) إنذار في أسبوع. كما أشار ما نسبته (١٥,٩٪) منهم بأن مؤسساتهم تتعرض إلى إنذارات بوجود جريمة عن طريق الإنترنت تصل من (١٠٠) إلى أقل من (١٠٠٠) إنذار في الأسبوع ، كما أشار ما نسبته (١٢,٨٪) منهم بأن مؤسساتهم تتعرض إلى إنذارات بوجود جريمة عن طريق الإنترنت تصل إلى أكثر من (١٠٠٠) إنذار في الأسبوع.

أوضحت الفقرة (١) السابقة ارتفاع معدل جرائم نظم المعلومات بعد ظهور الإنترنت (٤,٤٨) وهذا يتفق مع دراسة (Rapalus, ٢٠٠٢) ودراسة منظمة طوارئ الحاسب (CERT, ٢٠٠١) حيث أظهرت أنها تزداد معدلات ارتكاب الجرائم بزيادة استخدام الإنترنت، كما تتفق مع دراسة (المسند، والمهيني، ١٤٢١هـ)، التي ذكرت أن جرائم الحاسب الآلي مع وجود دعم الإنترنت وانتشارها السريع بهذا الشكل قد تمثل تهديداً مباشراً وفورياً وسريعاً للأمن الوطني والاقتصاد المحلي والعالمي، وانتهاكاً لحقوق الأفراد والمؤسسات على اختلاف أنواعها، وقد وجد المتسللون والمتطفلون ومحترفو الجرائم ضالتهم في الشبكة العالمية لممارسة جرائم التزوير واختلاس الأموال والقرصنة المعلوماتية، والتجسس

٦-٣-٣-٤ الأساليب المستخدمة في ارتكابها

يوضح جدول رقم (١٨) استجابة عينة الدراسة (العاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) والبالغ عددهم (١٠٥) فرداً حول تقييمهم لمدى استخدام كل أسلوب من الأساليب المستخدمة في ارتكاب جرائم نظم المعلومات بالمؤسسات (سواء من الداخل المؤسسة أو خارجها)، حيث يتضح إن أعلى الأساليب استخداماً إرسال الفيروسات بالبريد الإلكتروني، حيث

بلغت قيمة المتوسط الحسابي Mean (٤,٥٢)، وأقلها استخداماً زراعة برامج اختراق بواسطة موظفي الصيانة، حيث بلغت قيمة المتوسط الحسابي Mean (١,٩٨). أما حسب تقارب إجابات العينة يتضح إنهم أكثر تقارباً عند اعتراض الرسائل والتنصت حيث بلغ الانحراف المعياري Std.Deviation (٠,٦٢)، وأقلها تقارباً عند النفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثور على ملفات مشاركة غير محمية حيث بلغ الانحراف المعياري Std.Deviation (١,٧٢)، وقد جاءت النتائج على الترتيب (مرتبة حسب حجم حدوثها بالمؤسسات):

١. أوضح ما نسبته (٧٩,٠٪) من عينة الدراسة بأن حجم إرسال وزراعة الفيروسات عالي, مقابل ما نسبته (٣,٨٪) أوضحوا بأن حجم استخدام هذا الأسلوب محدود. وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٥٢) ويمثل نسبة قدرها (٩٠,٤٪)، وهذا يشير إلى أن حجم أسلوب إرسال وزراعة الفيروسات بالمؤسسات عالي جداً، (وهذا يتوافق مع ما تم التوصل إليه في جدول رقم ١٤)، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩١) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. أفاد ما نسبته (٨٠,٠٪) من عينة الدراسة بأن حجم إرفاق أحصنة طروادة بالبرامج عالي, مقابل ما نسبته (٩,٥٪) أفادوا بأن حجم استخدام هذا الأسلوب محدود، وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٢١) ويمثل نسبة قدرها (٨٤,٢٪)، وهذا يشير إلى أن حجم إرفاق أحصنة طروادة بالبرامج بالمؤسسات عالي جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٧) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٣. أوضح ما نسبته (٧٣,٤٪) من عينة الدراسة بأن حجم النفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثور على ملفات مشاركة غير محمية عالي، مقابل ما نسبته (١,٠٪) أوضحوا بأن حجم استخدام هذا الأسلوب محدود، وما نسبته (٢٥,٧٪) أوضحوا بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٧) ويمثل نسبة

قدرها (٧٧,٤٪)، وهذا يشير إلى أن حجم النفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثور على ملفات مشاركة غير محمية عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٧٢) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٤. أشار ما نسبته (٧٢,٤٪) من عينة الدراسة بأن حجم محاولة اكتشاف المنافذ المفتوحة والدخول منها عالي, مقابل ما نسبته (٢٧,٦٪) أشاروا بأن حجم استخدام هذا الأسلوب محدود، وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٧٤) ويمثل نسبة قدرها (٧٤,٢٪)، وهذا يشير إلى أن حجم محاولة اكتشاف المنافذ المفتوحة والدخول منها بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٦) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٥. أفاد ما نسبته (٦٤,٨٪) من عينة الدراسة بأن حجم محاولة اكتشاف المنافذ المفتوحة والدخول منها عالي, مقابل ما نسبته (١٦,٢٪) أفادوا بأن حجم استخدام هذا الأسلوب محدود، وما نسبته (١٧,١٪) أفادوا بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٧٤) ويمثل نسبة قدرها (٧٤,٢٪)، وهذا يشير إلى أن حجم محاولة اكتشاف المنافذ المفتوحة والدخول منها بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٦٦) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٦. أشار ما نسبته (٦٢,٨٪) من عينة الدراسة بأن حجم IP Spoofing عالي، مقابل ما نسبته (١٧,١٪) أشاروا بأن حجم استخدام هذا الأسلوب محدود. وقد حاز على الترتيب السادس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٦٥) ويمثل نسبة قدرها (٧٣,٠٪)، وهذا يشير إلى أن حجم IP Spoofing بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٨)، إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٧. أوضح ما نسبته (٦٢,٩٪) من عينة الدراسة بأن حجم استغلال الثغرات الأمنية في مزودات web مثل مزود IIS عالي, مقابل ما نسبته (٣٢,٤٪) أوضحوا بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٥٩) ويمثل نسبة قدرها (٧١,٨٪)، وهذا يشير إلى أن حجم استغلال الثغرات الأمنية في مزودات web مثل مزود IIS بالمؤسسات عالي، كما يشير الانحراف المعياري والبالغ قدرة (١,٨٥) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٨. أفاد ما نسبته (٦٣,٨٪) من عينة الدراسة بأن حجم استخدام برامج حديثة تقوم باستغلال نقاط الضعف في برامج الحماية عالي، مقابل ما نسبته (٢٩,٥٪) أفادوا بأن حجم استخدام هذا الأسلوب محدود، وما نسبته (٦,٧٪) أفادوا بأنه لا يستخدم. وقد حاز على الترتيب الثامن، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٥٠) ويمثل نسبة قدرها (٧٠,٠٪)، وهذا يشير إلى أن حجم استخدام برامج حديثة تقوم باستغلال نقاط الضعف في برامج الحماية بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٣٥) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٩. يرى ما نسبته (٦١,٩٪) من عينة الدراسة بأن حجم استغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة عالي, مقابل ما نسبته (٣٢,٤٪) يرون بأن حجم استخدام هذا الأسلوب محدود، وما نسبته (٥,٧٪) يرون بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب التاسع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٤٧) ويمثل نسبة قدرها (٦٩,٤٪)، وهذا يشير إلى أن حجم استغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة بالمؤسسات عالي، كما يشير الانحراف المعياري والبالغ قدرة Std.Deviation (١,٣٥) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٠. أوضح ما نسبته (٣١,٤٪) من عينة الدراسة بأن حجم ترك أقراص مرنة ملوثة بالفيروسات عالي, مقابل ما نسبته (٩,٥٪) أوضحوا بأن حجم استخدام هذا الأسلوب محدود، وما نسبته (٣,٨٪) أوضحوا بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب العاشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,١٨) ويمثل نسبة قدرها (٦٣,٦٪)، وهذا يشير إلى أن حجم ترك أقراص مرنة ملوثة بالفيروسات بالمؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٠) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

١١. أشار ما نسبته (٦٤,٨٪) من عينة الدراسة بأن حجم برمجة النظم والتطبيقات بطريقة تحقق للمبرمج مصالح شخصية غير مشروعة عالي، مقابل ما نسبته (٣٥,٢٪) أشاروا بأن حجم استخدام هذا الأسلوب محدود، وقد حاز على الترتيب الحادي عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٩٤) ويمثل نسبة قدرها (٥٨,٨٪)، وهذا يشير إلى أن حجم برمجة النظم والتطبيقات بطريقة تحقق للمبرمج مصالح شخصية غير مشروعة بالمؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٤٤) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٢. أشار ما نسبته (٣٥,٣٪) من عينة الدراسة بأن حجم سرقة وسائط الحفظ الخارجية نتيجة تساهل العاملين بالمؤسسة عالي, مقابل ما نسبته (٣٨,١٪) أشاروا بأن حجم استخدام هذا الأسلوب محدود، وقد حاز على الترتيب الثاني عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٩٣) ويمثل نسبة قدرها (٥٨,٦٪)، وهذا يشير إلى أن حجم سرقة وسائط الحفظ الخارجية نتيجة تساهل العاملين بالمؤسسة متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٧١) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٣. أبدا ما نسبته (٣٢,٤٪) من عينة الدراسة بأن حجم التخفي تحت البرامج المجانية والمواقع الجذابة للحصول على معلومات عن الزائر عالي، مقابل ما نسبته (٢٨,٦٪) أبدوا بأن حجم

استخدام هذا الأسلوب محدود، وما نسبته (٦,٧٪) أبدوا بأن هذا الأسلوب لا يستخدم، وقد حاز على الترتيب الثالث عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٩٠) ويمثل نسبة قدرها (٥٨,٠٪)، وهذا يشير إلى أن التخفي تحت البرامج المجانية والمواقع الجذابة للحصول على معلومات عن الزائر متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٤) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

١٤. أفاد ما نسبته (٤٣,٨٪) من عينة الدراسة بأن حجم الاستخدام غير القانوني لأجهزة غير حين تركها غير مؤمنة عالي, مقابل ما نسبته (٢٢,٩٪) أفادوا بأن حجم استخدام هذا الأسلوب محدود، وما نسبته (٢٥,٧٪) بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب الرابع عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٧٤) ويمثل نسبة قدرها (٥٤,٨٪)، وهذا يشير إلى أن الاستخدام غير القانوني لأجهزة غير حين تركها غير مؤمنة متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٣٤) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٥. أوضح ما نسبته (٣٢,٤٪) من عينة الدراسة بأن حجم إرفاق الملفات (ذاتية التشغيل/ بحاجة إلى تشغيل) والتي تقوم بعمليات تخريبية عالي، مقابل ما نسبته (٦,٧٪) أوضحوا بأن حجم استخدام هذا الأسلوب محدود, وما نسبته (٢٨,٦٪) أوضحوا بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب الخامس عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٦٩) ويمثل نسبة قدرها (٥٣,٨٪)، وهذا يشير إلى أن حجم إرفاق الملفات (ذاتية التشغيل/ بحاجة إلى تشغيل) والتي تقوم بعمليات تخريبية بالمؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٠) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٦. أفاد ما نسبته (٣٢,٤٪) من عينة الدراسة بأن حجم انتحال شخصية عبر البريد الإلكتروني عالي، مقابل ما نسبته (٥,٧٪) أفادوا بأن حجم استخدام هذا الأسلوب محدود, وما نسبته

(٣٠,٥٪) أفادوا بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب السادس عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٦٦) ويمثل نسبة قدرها (٥٥,٠٪)، وهذا يشير إلى أن حجم انتحال شخصية عبر البريد الإلكتروني متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٢) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٧. أدلى ما نسبته (٨,٦٪) من عينة الدراسة بأن حجم الحصول على البيانات السرية خلال صيانة الأجهزة عالي، مقابل ما نسبته (١١,٤٪) أدلوا بأن حجم استخدام هذا الأسلوب محدود، وما نسبته (٢٥,٧٪) أدلوا بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب السابع عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٤٦) ويمثل نسبة قدرها (٤٩,٢٪)، وهذا يشير إلى أنه من النادر الحصول على البيانات السرية خلال صيانة الأجهزة، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

١٨. يعد ما نسبته (٣٥,٢٪) من عينة الدراسة بأن حجم استخدام أسلوب تشغيل الجهاز عن طريق القرص المرن للدخول غير مرخص على الأقراص الثابتة والحصول على البيانات غير المؤمنة محدود. وقد حاز على الترتيب الثامن عشر، حيث بلغت قيمة المتوسط الحسابيMean (٢,٣٠) ويمثل نسبة قدرها (٤٦,٠٪)، وهذا يشير إلى أنه من النادر تشغيل الجهاز عن طريق القرص المرن للدخول غير مرخص على الأقراص الثابتة والحصول على البيانات غير المؤمنة بالمؤسسات، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٦) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

١٩. يرى ما نسبته (١,٠٪) من عينة الدراسة بأن حجم زراعة برامج اختراق بواسطة موظفي الصيانة عالي، مقابل ما نسبته (٣٨,١٪) يرون بأن حجم استخدام هذا الأسلوب محدود، وما نسبة (٣٢,٤٪) يرون بأن هذا الأسلوب لا يستخدم. وقد حاز على الترتيب التاسع عشر، حيث

بلغت قيمة المتوسط الحسابي Mean (١,٩٨) ويمثل نسبة قدرها (٣٩,٦٪)، وهذا يشير إلى أن حجم زراعة برامج اختراق بواسطة موظفي الصيانة بالمؤسسات محدود، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٩). إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

ويستنتج مما سبق أن هناك أساليب حجم استخدامها نحو نظم المعلومات بالمؤسسات (سواء من الداخل المؤسسة أو خارجها) عالي، وهي على الترتيب؛ إرسال الفيروسات بالبريد الإلكتروني أو برامج المحادثة وما شابهها (٤,٥٢)، إرفاق أحصنة طروادة بالبرامج (٤,٢١)، والنفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثور على ملفات مشاركة غير محمية (٣,٨٧)، واستغلال الثغرات التي تكتشف في نظم التشغيل والتطبيقات العاملة معه (٣,٧٤)، ومحاولة اكتشاف المنافذ المفتوحة والدخول منها (٣,٧٤)، وIP Spoofing (٣,٦٥)، واستغلال الثغرات الأمنية في مزودات web مثل مزود IIS (٣,٥٩)، واستخدام برامج حديثة تقوم باستغلال نقاط الضعف في برامج الحماية واستغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة (٣,٥٠). واستغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة (٣,٤٧).

ويتفق هذا جزئياً مع دراسة (المنشاوي، ١٤٢٤هـ) باستعراضه لبعض الأساليب كاجتياز مستخدمي الإنترنت بالمملكة البروكسي حيث يسلك هذا الأسلوب ما نسبته (٤١,٢٪)، واستخدامهم برامج إخفاء الشخصية أثناء تصفح الإنترنت بما نسبته (٢٠,٣٪)، ويتم استخدام برامج إخفاء الشخصية أثناء إرسال البريد الإلكتروني من قبلهم بما نسبته (١١,٨٪)، أما انتحال شخصية الآخرين أثناء التصفح أو إرسال البريد الإلكتروني فهذه الدراسة بينت أن المؤسسات تتعرض لما نسبته (٣٢,٤٪) بهذا الأسلوب، أما دراسة (المنشاوي) بينت أن ما نسبته (١١,٧٪) من قبل مستخدمي الإنترنت يسلكون هذا الأسلوب وهذا مقارب لحدٍ ما.

٦-٣-٣-٥ منافذ المؤسسة المستخدمة في ارتكابها

يوضح جدول رقم (١٩) استجابة عينة المحققين بالأجهزة الأمنية والعاملين في مجال نظم المعلومات إزاء حجم استخدام المنافذ الداخلية والخارجية للمؤسسة في ارتكاب جرائم نظم المعلومات بالمؤسسات، ولقد كانت النتائج على النحو التالي:

١. أوضح ما نسبته (٧٧,٩٪) من عينة الدراسة بأن حجم ارتكاب الجرائم عن طريق شبكة الإنترنت وبرامج الاختراق الموجودة بها عالي, مقابل ما نسبته (٢٠,٦٪) أوضحوا بأن حجم استخدام ذلك المنفذ محدود. وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٢٥) ويمثل نسبة قدرها (٨٥,٠٪)، وهذا يشير إلى أن حجم استخدام شبكة الإنترنت وبرامج الاختراق الموجودة بها كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات عالي جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢١) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٢. كشف ما نسبته (٦٦,٢٪) من عينة الدراسة بأنه يتم ارتكاب الجرائم عن طريق إفشاء الرقم السري من قبل الموظفين بشكل عالي, مقابل ما نسبته (٥,٩٪) كشفوا بأن هذا المنفذ لا يستخدم. وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,١٦) ويمثل نسبة قدرها (٨٣,٢٪)، وهذا يشير إلى أن حجم استخدام إفشاء الرقم السري من قبل الموظفين كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات عالي جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٩) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٣. يرى ما نسبته (٨٠,٩٪) من عينة الدراسة بأن حجم ارتكاب الجرائم عن طريق المحاولة المتكررة عالي, مقابل ما نسبته (٧,٤٪) يرون حجم استخدام ذلك المنفذ محدود، وما نسبته (٥,٩٪) بأن هذا المنفذ لا يستخدم. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط

الحسابي Mean (٣,٩٥) ويمثل نسبة قدرها (٧٩,٠٪)، وهذا يشير إلى أن حجم استخدام المحاولة المتكررة كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٩) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٤. أوضح ما نسبته (٦٣,٢٪) من عينة الدراسة بأنه يتم ارتكاب الجرائم عن طريق الأجهزة ومحركات الأقراص المرنة والليزر بشكل عالي, مقابل ما نسبته (٤,٤٪) بأن حجم استخدام ذلك المنفذ محدود، وما نسبته (١,٥٪) أوضحوا بأن هذا المنفذ لا يستخدم. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٩١) ويمثل نسبة قدرها (٧٨,٢٪)، وهذا يشير إلى أن حجم استخدام الأجهزة ومحركات الأقراص المرنة والليزر كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٠٣) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٥. يرى ما نسبته (٧٠,٦٪) من عينة الدراسة بأن حجم ارتكاب الجرائم عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد في ارتكاب الجرائم عالي, مقابل ما نسبته (٢,٩٪) يرون بأن حجم استخدام ذلك المنفذ محدود. وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٨) ويمثل نسبة قدرها (٧٧,٦٪)، وهذا يشير إلى أن حجم استخدام الشبكة المحلية LAN وبرامج التشارك في الموارد كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٦. كشف ما نسبته (٤٥,٦٪) من عينة الدراسة بأن حجم ارتكاب الجرائم عن طريق الشبكة الواسعة عالي, مقابل ما نسبته (٢٧,٩٪) كشفوا بأن حجم استخدام ذلك المنفذ محدود, وما نسبته (٥,٩٪) كشفوا بأن هذا المنفذ لا يستخدم. وقد حاز على الترتيب السادس، حيث بلغت قيمة المتوسط

الحسابي Mean (٣,٠٦) وهذا يشير إلى أن طريق شبكة الإنترنت وبرامج الاختراق الموجودة بها كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات عالي, كما يشير الانحراف المعياري والبالغ قدرة (١,٠٣) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٧. أشار ما نسبته (٤٥,٦٪) من عينة الدراسة بأن حجم ارتكاب الجرائم عن طريق برامج فك التشفير عالي، مقابل ما نسبته (٤,٤٪) أشاروا بأن حجم استخدام ذلك المنفذ محدود, وما نسبته (٥,٩٪) أشاروا بأن هذا المنفذ لا يستخدم. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٨٨) ويمثل نسبة قدرها (٥٧,٦٪)، وهذا يشير إلى أن حجم استخدام طريق استخدام برامج فك التشفير كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٥) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

٨. أشار ما نسبته (٣٦,٨٪) من عينة الدراسة بأن حجم ارتكاب الجرائم عن طريق شبكة VPN والبرامج التي تعمل عليها عالي، مقابل ما نسبته (١٩,١٪) أشاروا بأن حجم استخدام ذلك المنفذ محدود، وما نسبته (٣٦,٨٪) أشاروا بأن هذا المنفذ لا يستخدم. وقد حاز على الترتيب الثامن، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٤٤) ويمثل نسبة قدرها (٤٨,٨٪)، وهذا يشير إلى أن حجم استخدام شبكة VPN والبرامج التي تعمل عليها كمنفذ في ارتكاب جرائم نظم المعلومات بالمؤسسات محدود، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٣٢) إلى عدم تقارب وتركز إجابات عينة الدراسة وتشتتها.

ويستنتج مما سبق أن حجم استخدام منفذ شبكة الإنترنت وبرامج الاختراق الموجودة بها (٤,٢٥) (كمنفذ خارجي أعلى من حجم استخدام المنافذ الداخلية والخارجية الأخرى كإفشاء الرقم السري من قبل الموظفين (٤,١٦)، أو المحاولة المتكررة (٣,٩٥)، أو عن طريق الأجهزة

ومحركات الأقراص المرنة والليزر (٣,٩٥)، أو عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد (٣,٩١)، أو الشبكة الواسعة WAN والبرامج المرتبطة (٣,٨٨).

٦-٣-٣-٦ الأدوات المستخدمة من قبل مجرميها

يوضح جدول رقم (٢٠) استجابة عينة الدراسة (العاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) والبالغ عددهم (١٠٥) أفراد حول تقييمهم لمدى استخدام كل أداة من أدوات ارتكاب جرائم نظم المعلومات التي تتعرض لها المؤسسات (سواء من داخل المؤسسة أو خارجها)، حيث يتضح إن أعلى الأدوات استخداماً الفيروسات وديدان الإنترنت بمتوسط يبلغ (٤,٥٣)، وأقلها استخداماً Revelation بمتوسط يبلغ (٢,٤٠). وقد جاءت النتائج على الترتيب (مرتبة حسب حجم استخدامها):

١. أوضح ما نسبته (٨١,٠٪) من عينة الدراسة بأن حجم استخدام الفيروسات وديدان الإنترنت كأداة ارتكاب جريمة نظم معلومات عالي. وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٥٣) ويمثل نسبة قدرها (٩٠,٦٪)، وهذا يشير إلى أن حجم استخدام الفيروسات وديدان الإنترنت كأداة ارتكاب جريمة نظم معلومات عالي جداً. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٠) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٢. أفاد ما نسبته (٩٠,٥٪) من عينة الدراسة بأن حجم استخدام Cookies كأداة ارتكاب جريمة نظم معلومات عالي. وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٥١) ويمثل نسبة قدرها (٩٠,٢٪)، وهذا يشير إلى أن حجم استخدام Cookies كأداة ارتكاب جريمة نظم معلومات عالي جداً. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٧) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٣. أوضح ما نسبته (٦٤,٧٣٪) من عينة الدراسة بأن حجم استخدام البريد الإلكتروني كأداة ارتكاب جريمة نظم معلومات عالي. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٤,١٨) ويمثل نسبة قدرها (٨٣,٦٪)، وهذا يشير إلى أن حجم استخدام البريد الإلكتروني كأداة ارتكاب جريمة نظم معلومات عالي جداً. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٣) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٤. أشار ما نسبته (٧١,٤٪) من عينة الدراسة بأن حجم استخدام المشاركة في الملفات على الشبكة عالي، مقابل ما نسبته (٥,٧٪) أشاروا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean بمتوسط يبلغ (٤,٠٨) ويمثل نسبة قدرها (٨١,٦٪)، وهذا يشير إلى أن حجم استخدام المشاركة في الملفات على الشبكة كأداة ارتكاب جريمة نظم معلومات عالي. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٤) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٥. أوضح ما نسبته (٥٨,١٪) من عينة الدراسة بأن حجم استخدام برامج التنصت على الشبكات كأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (٤,٨٪) أوضحوا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٩) ويمثل نسبة قدرها (٧٧,٨٪)، وهذا يشير إلى أن حجم استخدام برامج التنصت على الشبكات كأداة ارتكاب جريمة نظم معلومات عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٥) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٦. يرى ما نسبته (٧١,٥٪) من عينة الدراسة بأن حجم استخدام برنامج Net Busكأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (١٨,١٪) يرون بأن حجم استخدام هذه الأداة محدود، وما نسبته (١,٩٪) يرون بأن هذا البرنامج لا يستخدم. وقد حاز على الترتيب

السادس، حيث بلغت قيمة المتوسط الحسابي Mean بمتوسط يبلغ (٣,٨٠) ويمثل نسبة قدرها (٧٦,٠٪)، وهذا يشير إلى أن حجم استخدام برنامج Net Bus كأداة ارتكاب جريمة نظم معلومات عالي. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٢) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٧. أفاد ما نسبته (٥٩,٥٪) من عينة الدراسة بأن حجم استخدام برنامج Sub Seven كأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (٢٢,٩٪) أفادوا بأن حجم استخدام هذه الأداة محدود، وما نسبته (١,٩٪) أفادوا بأن هذا البرنامج لا يستخدم. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٧٥) ويمثل نسبة قدرها (٧٥,٠٪)، وهذا يشير إلى أن حجم استخدام برنامج Sub Seven كأداة ارتكاب جريمة نظم معلومات عالي. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٩) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٨. أوضح ما نسبته (٣٩,٠٪) من عينة الدراسة بأن حجم استخدام برنامج ICQ عالي, مقابل ما نسبته (٢٢,٩٪) أوضحوا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب الثامن، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٥١) ويمثل نسبة قدرها (٧٠,٢٪)، وهذا يشير إلى أن حجم استخدام برنامج ICQ كأداة ارتكاب جريمة نظم معلومات عالي. كما يشير الانحراف المعياري والبالغ قدرة (١,١٩) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٩. أشار ما نسبته (٥٥,٣٪) من عينة الدراسة بأن حجم استخدام برنامج Password Recovery Toolkit كأداة ارتكاب جريمة نظم معلومات عالي، مقابل ما نسبته (٣٣,٣٪) أشاروا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب التاسع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٤٦) ويمثل نسبة قدرها (٦٩,٢٪)، وهذا يشير إلى أن حجم استخدام

Password Recovery Toolkit كأداة ارتكاب جريمة نظم معلومات عالي، كما يشير الانحراف المعياري والبالغ قدرة Std.Deviation (١,١٩) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

١٠. أوضح ما نسبته (٣٧,١٪) من عينة الدراسة بأن حجم استخدام برنامج Tribe Flood Network كأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (٣٠,٥٪) أوضحوا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب العاشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٢٩) ويمثل نسبة قدرها (٦٥,٨٪)، وهذا يشير إلى أن حجم استخدام Network Tribe Floodكأداة ارتكاب جريمة نظم معلومات بدرجة كبيرة، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١٢) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

١١. ذكر ما نسبته (٤٣,٨٪) من عينة الدراسة بأن حجم استخدام برنامج Hack a Tack كأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (٣٢,٤٪) ذكروا بأن حجم استخدام هذه الأداة محدود، وما نسبته (١,٩٪) ذكروا بأن هذا البرنامج لا يستخدم. وقد حاز على الترتيب الحادي عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,١٩) ويمثل نسبة قدرها (٣٦,٨٪)، وهذا يشير إلى أن حجم استخدام برنامج Hack a Tack كأداة ارتكاب جريمة نظم معلومات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٠٨) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

١٢. أفاد ما نسبته (٣٦,٢٪) من عينة الدراسة بأن حجم استخدام برنامج Win Crash كأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (٢٥,٧٪) أفادوا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب الثاني عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,١٦) ويمثل نسبة قدرها (٦٣,٢٪)، وهذا يشير إلى أن حجم استخدام برنامجWin Crash كأداة ارتكاب جريمة نظم معلومات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٩) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

١٣. أوضح ما نسبته (٢٢,٩٪) من عينة الدراسة بأن حجم استخدام أقراص بدء التشغيل كأداة ارتكاب جريمة نظم معلومات عالي، مقابل ما نسبته (٢١,٩٪) أوضحوا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب الثالث عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٠١) ويمثل نسبة قدرها (٦٠,٢٪)، وهذا يشير إلى أن حجم استخدام أقراص بدء التشغيل كأداة ارتكاب جريمة نظم معلومات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٧) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

١٤. أوضح ما نسبته (٩,٥٪) من عينة الدراسة بأن حجم استخدام برنامج MS Word Cracker كأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (٣٣,٣٪) أوضحوا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب الرابع عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٠١) ويمثل نسبة قدرها (٦٠,٢٪)، وهذا يشير إلى أن حجم استخدام برنامج MS Word Cracker كأداة ارتكاب جريمة نظم معلومات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٤) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

١٥. كشف ما نسبته (٢٤,٧٪) من عينة الدراسة بأن حجم استخدام برنامج MS Excel Cracker كأداة ارتكاب جريمة نظم معلومات عالي, مقابل ما نسبته (٣٢,٤٪) كشفوا بأن حجم استخدام هذه الأداة محدود. وقد حاز على الترتيب الخامس عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٨٨) ويمثل نسبة قدرها (٥٧,٦٪)، وهذا يشير إلى أن حجم استخدام برنامج MS Excel Cracker كأداة ارتكاب جريمة نظم معلومات متوسط. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٥) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

١٦. يرى ما نسبته (٢٦,٧٪) من عينة الدراسة بأن حجم استخدام برنامج Caligula كأداة ارتكاب جريمة نظم معلومات عالي، مقابل ما نسبته (٣٥,٢٪) يرون بأن حجم استخدام هذه الأداة

محدود, وما نسبته (٧,٦٪) يرون بأن هذا البرنامج لا يستخدم، وقد حاز على الترتيب السادس عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٧٦) ويمثل نسبة قدرها (٥٥,٢٪)، وهذا يشير إلى أن حجم استخدام برنامج Caligula كأداة ارتكاب جريمة نظم معلومات متوسط. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٤) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

١٧. أفاد ما نسبته (٢٥,٧٪) من عينة الدراسة بأن حجم استخدام برنامج Marker Groove كأداة ارتكاب جريمة نظم معلومات عالي، مقابل ما نسبته (٣٥,٢٪) أفادوا بأن حجم استخدام هذه الأداة محدود، وما نسبته (٩,٥٪) أفادوا بأن هذا البرنامج لا يستخدم. وقد حاز على الترتيب السابع عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٧١) ويمثل نسبة قدرها (٥٤,٢٪)، وهذا يشير إلى أن حجم استخدام برنامج Marker Groove كأداة ارتكاب جريمة نظم معلومات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٦) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

١٨. أوضح ما نسبته (٥,٧٪) من عينة الدراسة بأن حجم استخدام برنامج Revelation كأداة ارتكاب جريمة نظم معلومات عالي، مقابل ما نسبته (٦٢,٩٪) أوضحوا بأن حجم استخدام هذه الأداة محدود, وما نسبته (١,٠٪) أوضحوا بأن هذا البرنامج لا يستخدم. وقد حاز على الترتيب الثمن عشر والأخير، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٤٠) ويمثل نسبة قدرها (٤٨,٠٪)، وهذا يشير إلى أن حجم استخدام برنامج Revelation كأداة ارتكاب جريمة نظم معلومات محدود، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٢) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

ويستنتج مما سبق أن هناك أدوات حجم استخدامها بالمؤسسات عالي، وهي على الترتيب؛ الفيروسات وديدان الإنترنت (٤,٥٣)، وCookies (٤,٥١)، والبريد الإلكتروني (٤,١٨)،

والمشاركة في الملفات على الشبكة (٤,٠٨)، برامج التنصت على الشبكات (٣,٨٩)، برنامج Net Bus(٣,٨٠)، وبرنامج Sub Seven (٣,٧٥)، وبرنامج ICQ (٣,٥١)، وبرنامج Password Recovery Toolkit (٣,٤٦)، وبرنامج Tribe Flood Network (٣,٢٩).

٦-٣-٣-٧ كيفية وحجم الحصول علي أدوات ارتكابها بالمملكة

يوضح جدول رقم (٢١) استجابة عينة الدراسة (العاملين في مجال نظم المعلومات وموفري تقنيات أمن النظم) والبالغ عددهم (١٠٥) أفراد حول تقييمهم لكيفية وحجم الحصول على أدوات ارتكاب جرائم نظم المعلومات حيث جاءت إجابات عينة الدراسة على النحو التالي:

١. أوضحت إجابات عينة الدراسة بأنهم يوافقون بنسبته (١٠٠٪) على أن حجم الحصول على برامج مجانية تستخدم لارتكاب جرائم نظم المعلومات من مواقع على شبكة الإنترنت عالي، وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٩٦) ويمثل نسبة قدرها (٩٩,٢٪)، وهذا يشير إلى أن حجم الحصول على البرامج المجانية المستخدمة لارتكاب جرائم نظم المعلومات من مواقع على شبكة الإنترنت كبير جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,١٩) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٢. أظهرت إجابات عينة الدراسة بأنهم يوافقون بنسبته (١٠٠٪) على أن حجم الحصول على برامج تستخدم لارتكاب جرائم نظم المعلومات من أماكن البيع غير القانونية للبرامج عالي، وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٧١) ويمثل نسبة قدرها (٩٤,٢٪)، وهذا يشير إلى أن حجم الحصول على البرامج المستخدمة لارتكاب جرائم نظم المعلومات من أماكن البيع غير القانونية كبير جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٤٥) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٣. أوضح ما نسبته (٦٦,٧٪) من عينة الدراسة بأن حجم الحصول على البرامج غير مجانية التي تشترى من مواقع على شبكة الإنترنت عالي. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٦٦) ويمثل نسبة قدرها (٧٣,٢٪)، وهذا يشير إلى أنه حجم الحصول على البرامج غير المجانية التي تشترى من مواقع على شبكة الإنترنت كبير، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٤٧) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٤. أوضح ما نسبته (١٧,١٪) من عينة الدراسة بأن حجم الحصول على أدوات ارتكاب الجريمة من محلات بيع البرامج المرخصة عالي، مقابل (٦,٧٪) بأن حجم الحصول تلك الأدوات المستخدمة بارتكاب جرائم نظم المعلومات محدود, وما نسبته (٢٦,٧٪) ليس لديهم علم بذلك. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٥٧) ويمثل نسبة قدرها (٥١,٤٪)، وهذا يشير إلى أن حجم الحصول على برامج أدوات ارتكاب الجريمة من محلات بيع البرامج المرخصة متوسط. كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٠٦) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٦-٣-٣-٨ مستوى مكافحتها

يوضح جدول رقم (٢٢) استجابة عينة الدراسة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات) إزاء مستوى مكافحة جرائم نظم المعلومات وكانت النتائج على النحو التالي:

١. يرى ما نسبته (٧٥,٠٪) من عينة الدراسة بأن قدر الجهد المبذول لمتابعة جرائم نظم المعلومات من قبل قسم خاص بالمؤسسة عالي، مقابل ما نسبته (٢٠,٠٪) بأن حجم ذلك الجهد محدود. وقد بلغت قيمة المتوسط الحسابي Mean (٣,٩٦) ويمثل نسبة قدرها (٧٩,٢٪)، وهذا يشير إلى أن

قدر الجهد المبذول لمتابعة جرائم نظم المعلومات من قبل قسم خاص بالمؤسسة عالي، كما يشير الانحراف المعياري والبالغ قدرة (١,١٣) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٢. أفاد ما نسبته (٤٣,٢٪) من عينة الدراسة بأن حجم الاعتماد على ضمانات موردي الأجهزة والبرامج بدلاً من تتبع الجرائم عالي، مقابل ما نسبته (٧,٧٪) أفادوا بأن حجم ذلك الاعتماد محدود. وقد بلغت قيمة المتوسط الحسابي Mean (٣,٣٨) ويمثل نسبة قدرها (٦٧,٦٪)، وهذا يشير إلى أن حجم الاعتماد على ضمانات موردي الأجهزة والبرامج بدلاً من تتبع الجرائم عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٦) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٣. أفاد ما نسبته (٣٠,٨٪) من عينة الدراسة بأن حجم جرائم نظم المعلومات التي اكتشفت وضبطت ملابساتها عالي، مقابل ما نسبته (١٩,٢٪) أفادوا بأن حجمها محدود، وما نسبته (٢,٩٪) أفادوا بأنها لم تضبط. وقد بلغت قيمة المتوسط الحسابي Mean (٣,٠٦) ويمثل نسبة قدرها (٦١,٢٪)، وهذا يشير إلى أن حجم جرائم نظم المعلومات التي اكتشفت وضبطت ملابساتها متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨١) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٤. أشار ما نسبته (٣٢,٧٪) من عينة الدراسة بأن حجم الجرائم التي تم ضبطها ومعرفة مصدرها وآثارها في مؤسساتهم عالي، مقابل ما نسبته (٢٥,٠٪) أشاروا بأن حجمها محدود، وما نسبته (١,٩٪) أشاروا بأنها لا توجد. وقد بلغت قيمة المتوسط الحسابي Mean (٣,٠٤) ويمثل نسبة قدرها (٦٠,٨٪)، وهذا يشير إلى أن حجم الجرائم التي تم ضبطها ومعرفة مصدرها وآثارها في المؤسسات متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨١) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٥. أبدا ما نسبته (٤١,٤٪) من عينة الدراسة بأن حجم اهتمام الجهة الأمنية بعد الإبلاغ عن الجريمة المعلوماتية عالي، مقابل ما نسبته (٢٦,٠٪) أبدوا بأن حجم اهتمامها محدود، وما نسبته (١٨,٣٪) أبدوا بأنه لا يوجد. وقد بلغت قيمة المتوسط الحسابي Mean (٢,٨٨) ويمثل نسبة قدرها (٥٧,٦٪)، وهذا يشير إلى أن حجم اهتمام الجهة الأمنية بعد الإبلاغ عن الجريمة المعلوماتية متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٩) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٦. يرى ما نسبته (١١,٥٪) من عينة الدراسة بأن حجم جرائم نظم المعلومات التي اكتشفت دون ضبط ملابساتها عالي، مقابل ما نسبته (٢٩,٨٪) يرون حجمها محدود، وما نسبته (٩,٦٪) يرونه لا يوجد، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٦٣) ويمثل نسبة قدرها (٥٢,٦٪)، وهذا يشير إلى أن حجم جرائم نظم المعلومات التي اكتشفت دون ضبط ملابساتها متوسط، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨١) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٦-٣-٣-٩ دوافعها

يوضح جدول رقم (٢٣) استجابة العينة (المحققين بالأجهزة الأمنية والعاملين في مجال نظم المعلومات) والبالغ عددهم (١٠٤) أفراد حول تقييمهم لدوافع جرائم نظم المعلومات، وجاءت النتائج على النحو التالي:

١. أفاد ما نسبته (٧٧,٩٪) من عينة الدراسة بأن حجم ارتكاب الجرائم بدافع التسلية وحب الاستطلاع عالي, مقابل ما نسبته (٢,٩٪) أفادوا بأنه لا يوجد، وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,١٩) ويمثل نسبة قدرها (٨٣,٨٪)، وهذا يشير إلى أن حجم تعرض المؤسسات لارتكاب جرائم نظم المعلومات بدافع التسلية وحب الاستطلاع عالي

جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٦) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٢. أشار ما نسبته (٩٦,٢٪) من عينة الدراسة بأن حجم ارتكاب الجرائم بدافع الوصول إلى معلومات شخصية عالي، مقابل ما نسبته (٥,٨٪) بأن حجم هذا الدافع محدود، وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٦) ويمثل نسبة قدرها (٨١,٠٪)، وهذا يشير إلى أن حجم تعرض المؤسسات لارتكاب جرائم نظم المعلومات بدافع الوصول إلى معلومات شخصية عالي جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٥) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٣. أوضح ما نسبته (٦٩,٢٪) من عينة الدراسة بأن حجم ارتكاب الجرائم لإبراز القدرات عالي، مقابل ما نسبته (٦,٧٪) أوضحوا بأن حجم هذا الدافع محدود. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٢) ويمثل نسبة قدرها (٨٠,٤٪)، وهذا يشير إلى أن حجم تعرض المؤسسات لارتكاب جرائم نظم المعلومات بدافع إبراز القدرات عالي جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٩٤) إلى تقارب وتركز إجابات العينة وعدم تشتتها.

٤. أوضح ما نسبته (٧٤,٠٪) من عينة الدراسة بأن حجم ارتكاب الجرائم بسبب الانتقام عالي, مقابل ما نسبته (٢,٩٪) أوضحوا بأن حجم هذا الدافع محدود، وما نسبته (١١,٥٪) أوضحوا بأنه لا يوجد. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٩٨)، وهذا يشير إلى أن حجم تعرض المؤسسات لارتكاب جرائم نظم المعلومات بدافع الانتقام عالي، كما يشير الانحراف المعياري والبالغ قدرة (١,٣٣) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٥. أشار ما نسبته (٥٥,٨٪) من عينة الدراسة بأن حجم ارتكاب الجرائم بدوافع اقتصادية وتجارية عالي, مقابل ما نسبته (٢١,٢٪) أشاروا بأن حجم هذه الدوافع محدود، وما نسبته (٧,٧٪) أوضحوا بأنه لا يوجد. وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٢٥) ويمثل نسبة قدرها (٦٥,٤٪)، وهذا يشير إلى أن تعرض المؤسسات لارتكاب جرائم نظم المعلومات بدوافع اقتصادية وتجارية عالي، كما يشير الانحراف المعياري والبالغ قدرة (١,٠٩) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

٦. أفاد ما نسبته (٢٧,٩٪) من عينة الدراسة بأن حجم الدوافع السياسية والعسكرية لارتكاب الجرائم عالي، مقابل ما نسبته (١٦,٣٪) أفادوا بأن حجم هذا الدافع محدود، وما نسبته (٤٩,٠٪) أفادوا بأنه لا يوجد. وقد حاز على الترتيب الأخير، حيث بلغت قيمة المتوسط الحسابي Mean (٢,١٣)، وهذا يشير إلى أنه من النادر أن تتعرض المؤسسات لارتكاب جرائم بدوافع سياسية وعسكرية، ويعزو الباحث ذلك بسبب عدم أهمية معلومات المؤسسات التي شملتها الدراسة إلى أن تستفيد منها جهة معينة لصالح أنشطتها السياسية والعسكرية، كما يشير الانحراف المعياري والبالغ قدرة (١,٢٩) إلى عدم تقارب وتركز إجابات العينة وتشتتها.

ويستنتج مما سبق أن حجم استخدام منفذ شبكة الإنترنت وبرامج الاختراق الموجودة بها (٤,٢٥) كمنفذ خارجي أعلى من المنافذ الداخلية والخارجية الأخرى كإفشاء الرقم السري من قبل الموظفين (٤,١٦)، أو المحاولة المتكررة (٣,٩٥)، أو عن طريق الأجهزة ومحركات الأقراص المرنة والليزر (٣,٩٥)، أو عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد (٣,٩١)، أو الشبكة الواسعة WAN والبرامج المرتبطة (٣,٨٨)، وهذا يختلف مع (الفنتوخ) بأن جرائم الحاسب الآلي الداخلية تشكل ما يقارب (٨٠٪) من الداخل. ويعزي الباحث هذا إلى الاعتماد على الشبكات وخصوصاً الإنترنت في أداء الأعمال.

٦-٣-٣-١٠ تكلفتها

يوضح جدول رقم (٢٤) استجابة عينة الدراسة (العاملين في مجال نظم المعلومات) حيال تكلفة جرائم نظم المعلومات في المؤسسات التي يعملون بها في عام ٢٠٠١م، حيث أظهر الجدول أن ما نسبته (٤٢,٦٪) من العينة أكدوا بأن تكلفة جرائم نظم المعلومات في المؤسسات التي يعملون بها لا تتجاوز (٥٪)، وما نسبته (٣٦,٨٪) أكدوا بأن تكلفتها من (٥٪) إلى أقل من (١٠٪)، وما نسبته (١٤,٧٪) منهم أكدوا بأن تكلفتها من (١٠٪) إلى أقل من (٣٠٪) وما نسبته (٤,٤٪) منهم أكدوا بأن تكلفتها من (٣٠٪) إلى (٥٠٪)، وواحد فقط ويمثل (١,٥٪) أكد بأن تكلفتها أكثر من (٥٠٪).

ويستنتج مما سبق أن جرائم نظم المعلومات تسببت لما نسبته (٤٢,٦٪) من مؤسسات عينة الدراسة بخسائر مادية تبلغ أقل من (٥٪) من نسبة أجمالي مصروفات المؤسسة. كما تسببت لما نسبته (٣٦,٨٪) من مؤسسات عينة الدراسة بخسائر مادية تبلغ من (٥٪) إلى أقل من (١٠٪) من نسبة أجمالي مصروفات المؤسسة. وتسببت لما نسبته (٢٠,٦٪) من مؤسسات عينة الدراسة بخسائر مادية تبلغ أكثر من (١٠٪) من نسبة أجمالي مصروفات المؤسسة. وهذا يتفق مع دراسة (Rapalus, ٢٠٠٢) حيث بين أن نسبة (٨٠٪) اعترفوا بخسائر مالية، كما أن نسبة (٤٤٪) (٢٢٣ من المجيبين) أفادوا عن خسائر بقيمة (٤٥٥،٨٤٨،٠٠٠) دولار في عام ٢٠٠١م.. كما يتفق مع دراسة (البداينة، ١٩٩٨م)، حيث قدر حجم الخسائر المادية لجرائم الحاسب الآلي في المملكة بحوالي (١١٢) مليون ريال سعودي في عام ١٤١٨هـ، كما قدرها في دراسة أخرى له (البداينة، ١٤٢٠هـ: ٤١) بحوالي (٥٦٢,٥) مليون ريال، أصابت العديد من المؤسسات والأفراد في المملكة خلال عام ١٤١٩هـ. ويعزي الباحث هذا بسبب الاعتماد الكبير على نظم المعلومات من قبل المؤسسات ومنها الإنترنت في أدى نشاطها، وبشكل عام يرجع إلى طبيعة هذه الجرائم والعوامل المؤثرة في سرعة انتشارها.

٦-٣-٤ وسائل التحقيق في جرائم نظم المعلومات

شملت هذه الفقرة عرض لاستجابة عينة الدراسة نحو الوسائل المستخدمة بضبط الجريمة، والوسائل المساعدة بضبط الجريمة، والوسائل المستخدمة بتحديد شخصية مرتكبها، والأدوات المساعدة بالتحقيق.

٦-٣-٤-١ الوسائل المستخدمة بضبط الجريمة

توضح الجداول التي أرقامها الأعداد (٢٥، ٢٦، ٢٧) استجابة عينة الدراسة (المحققين بالأجهزة الأمنية والعاملين في مجال نظم المعلومات) إزاء الوسائل المستخدمة بضبط الجريمة حيث جاءت النتائج على النحو التالي:

١. أكد ما نسبته (٨٧,٥٪) من عينة الدراسة إمكانية استخدام تقنية المعلومات كوسيلة من وسائل ضبط الجريمة غالباً، مقابل ما نسبته (٨,٧٪) أكدوا بإمكانية استخدامها أحياناً، وما نسبته (٣,٨٪) أكدوا بإمكانية استخدامها نادراً. وقد بلغت قيمة المتوسط الحسابي Mean (٤,١٦) ويمثل نسبة قدرها (٨٣,٤٪)، وهذا يشير إلى إمكانية استخدام تقنية المعلومات كوسيلة من وسائل ضبط الجريمة والتحقيق فيها بشكل دائم، كما يشير الانحراف المعياري والبالغ قدرة (٠,٧٤) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. يرى ما نسبته (٢١,٢٪) من عينة الدراسة أن برامج الحماية وسيلة ضبط وتحقيق هامة بشكل دائم، وما نسبته (٥٤,٨٪) يرونها غالباً وسيلة ضبط وتحقيق هامة، مقابل ما نسبته (١١,٥٪) يرونها أحياناً وسيلة ضبط وتحقيق هامة تكون ذلك. وقد بلغت قيمة المتوسط الحسابي Mean (٤,٥٠)، وهذا يشير إلى أن برامج الحماية تعد وسيلة ضبط وتحقيق هامة دائماً. كما يشير الانحراف المعياري والبالغ قدرة (٠,٧٠) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٣. أشار ما نسبته (٢١,٢٪) من عينة الدراسة بأنه دائماً يتم تحديد مصدر الهجوم (داخلي، خارجي)، وما نسبته (٥٥,٨٪) أشاروا بأنه غالباً يتم تحديده، مقابل ما نسبته (١٥,٤٪) أشاروا بأنه أحياناً يتم تحديده، وما نسبته (٧,٧٪) أشاروا بأنه نادراً يتم تحديده. وقد بلغت قيمة المتوسط الحسابي Mean (٣,٩٠)، ويمثل نسبة قدرها (٧٨,٤٪)، وهذا يشير إلى أنه غالباً تستطيع المؤسسة المستهدفة من قبل مجرمي نظم المعلومات تحديد مصدر الهجوم. كما يشير الانحراف المعياري والبالغ قدرة (٠,٨٢) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٤. كشف ما نسبته (١٣,٥٪) من عينة الدراسة بأنه دائماً يتم تحديد مصدر الأدوات المستخدمة في الهجوم، وما نسبته (٢٣,١٪) كشفوا بأنه غالباً يتم تحديده، مقابل ما نسبته (٣٢,٧٪) بأنه أحياناً يتم تحديده، وما نسبته (٣٠,٨٪) كشفوا بأنه نادراً ما يتم تحديده. وقد بلغت قيمة المتوسط الحسابي Mean (٣,٠١)، وهذا يشير إلى أنه أحياناً تستطيع المؤسسة المستهدفة من قبل مجرمي نظم المعلومات تحديد مصدر الأدوات المستخدمة في الهجوم. كما يشير الانحراف المعياري والبالغ قدرة (٠,٨١) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٥. أكد ت إجابات عينة الدراسة أن برامج الحماية تعد أحد الوسائل المستخدمة بالتحقيق وتقوم بعدد من الوظائف في ضبط الجريمة؛ فنسبة الذين ذكروا أنها تحدد نوع الجريمة فقط (١,٠٪)، وما نسبته (٥,٨٪) ذكروا أنها تحدد مصدر الجريمة فقط، وما نسبته (٢,٩٪) ذكروا أنها تحدد توقيت ارتكاب الجريمة فقط، وما نسبته (١,٠٪) ذكروا أنها تقوم بالإعلام عن وجود جريمة مرتكبة فقط، وما نسبته (١١,٥٪) ذكروا أنها تحدد نوع الجريمة وتوقيت ارتكابها، وما نسبته (١٦,٣٪) ذكروا أنها تحدد نوعها وتوقيت ارتكابها والإعلام بوجودها، وما نسبته (٧٢,١٪) ذكروا أنها تحدد نوعها ومصدرها وتوقيت ارتكابها والإعلام بوجودها. ويستنتج من هذا على أنه بالإمكان استخدام برامج الحماية بما نسبته (٩٤,٢٪) في تحديد نوع الجريمة، وما نسبته

(٩٥,١٪) في تحديد توقيت ارتكاب الجريمة، وما نسبته (٧٥٪) في تحديد مصدر الجريمة، وما نسبته (٩٤,٢٪) في الإعلام بوجود جريمة مرتكبة.

٦-٣-٤-٢ الأدوات المستخدمة بضبط الجريمة

يوضح جدول رقم (٢٨) استجابة عينة الدراسة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) والبالغ عددهم (١٤١) فرداً حول تقييمهم لمدى أهمية الأدوات المستخدمة بضبط الجريمة، ولقد جاءت النتائج على النحو التالي:

١. أكدت إجابات ما نسبته (٩٤,٣٪) من عينة الدراسة أن سجل الصلاحيات للمستخدمين مهم جداً، وما نسبته (٥,٧٪) منهم أكدت إجاباتهم بأنه مهم. وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٩٤) ويمثل نسبة قدرها (٩٨,٨٪). وهذا يشير إلى أن سجل الصلاحيات للمستخدمين كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٢٣) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. أوضح ما نسبته (٨٥,٨٪) من عينة الدراسة بأن التقارير التي تنتجها نظم أمن البيانات مهمة جداً، وما نسبته (١٤,٢٪) أوضحوا بأنه مهم، وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٨٦) ويمثل نسبة قدرها (٩٧,٠٪). وهذا يشير إلى أن التقارير التي تنتجها نظم أمن البيانات كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٣٥) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٣. يرى ما نسبته (٧٥,٩٪) من عينة الدراسة أن برامج النسخ الاحتياطي والتسجيل Logging مهمة جداً، وما نسبته (٢٤,١٪) يرونها مهمة. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٧٦) ويمثل نسبة قدرها (٩٥,٢٪)، وهذا يشير إلى أن برامج النسخ

الاحتياطي والتسجيل Logging كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٤٣) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٤. أفاد ما نسبته (٧٤,٥٪) من عينة الدراسة بأن برامج كشف الفيروسات مهمة جداً، وما نسبته (٢٥,٥٪) أفادوا بأنها مهمة، وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٧٤) ويمثل نسبة قدرها (٩٤,٨٪)، وهذا يشير إلى أن برامج كشف الفيروسات كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٤٢) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٥. أظهرت إجابات ما نسبته (٦٨,٨٪) من عينة الدراسة بأن أدوات المراجعة Auditing مهمة جداً، وما نسبته (٣١,٢٪) أظهرت بأنها مهمة، وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٦٩) ويمثل نسبة قدرها (٩٣,٨٪)، وهذا يشير إلى أن أدوات المراجعة Auditing كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٤٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٦. أشار ما نسبته (٥٥,٣٪) من عينة الدراسة بأن تقارير الجدران النارية مهمة جداً، وما نسبته (٤٢,٦٪) أشاروا بأنها مهمة، وقد حاز على الترتيب السادس، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٥٣) ويمثل نسبة قدرها (٩٣,٨٪)، وهذا يشير إلى أن تقارير الجدران النارية كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٥٤) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٧. يرى ما نسبته (٦٢,٤٪) من عينة الدراسة بأن أدوات مراقبة المستخدمين للشبكة مهمة جداً، وما نسبته (٢٧,٧٪) يرونها مهمة، وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابيMean (٤,٥٢) ويمثل نسبة قدرها (٩٠,٤٪)، هذا يشير إلى أن أدوات مراقبة

المستخدمين للشبكة مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٦٩) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٨. ذكر ما نسبته (٤١,٨٪) من عينة الدراسة أن برامج تتبع المخترقين مهمة جداً، وما نسبته (٢٩,٨٪) ذكروا بأنها مهمة، مقابل ما نسبته (٢,١٪) ذكروا بأنها غير مهمة، وقد حاز على الترتيب التاسع، حيث بلغت قيمة المتوسط الحسابي Mean (٤,١١) ويمثل نسبة قدرها (٨٢,٢٪)، وهذا يشير إلى أن برامج تتبع المخترقين كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٨٧) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٩. أشار ما نسبته (٣١,٢٪) من عينة الدراسة أن مراجعة قاعدة البيانات مهمة جداً، وما نسبته (٤٥,٤٪) أشاروا بأنها مهمة، وقد حاز على الترتيب العاشر، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٧) ويمثل نسبة قدرها (٦٦,٤٪)، وهذا يشير إلى أن مراجعة قاعدة البيانات كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٧٣) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها..

١٠. يرى ما نسبته (٤٠,٤٪) من عينة الدراسة أن برامج تتبع مصدر الرسائل مهمة جداً، ما نسبته (٣٣,٣٪) يرونها مهمة، مقابل ما نسبته (٢,١٪) يرونها غير مهمة. وقد حاز على الترتيب الحادي عشر، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٦) ويمثل نسبة قدرها (٨١,٢٪). وهذا يشير إلى أن برامج تتبع مصدر الرسائل كأداة ضبط مهمة جداً، كما يشير الانحراف المعياري والبالغ قدرة (٠,٩٥) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٦-٣-٤-٣ الوسائل المستخدمة بتحديد شخصية مرتكبها

يظهر الجدولين رقم (٢٩، ٣٠) استجابة عينة الدراسة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات) والبالغ عددهم (١٠٤) أفراد إزاء الوسائل المستخدمة لتحديد شخصية مرتكب جريمة نظم المعلومات، وكانت النتائج على النحو التالي:

١. يرى ما نسبته (٤,٨٪) من عينة الدراسة أنه يمكن تحديد شخصية مرتكب جريمة نظم المعلومات بعنوانIP فقط، وما نسبته (٢,٩٪) يرون أنه يمكن تحديده بواسطة برامج الحماية فقط، وما نسبته (١,٩٪) يرون أنه يمكن تحديده بواسطة وسائل تتبع المخترقين فقط، وما نسبته (١,٠٪) يرون أنه يمكن تحديده بواسطة برامج تتبع مصدر الرسائل فقط، وما نسبته (١٠,٦٪) يرون أنه يمكن تحديده بواسطة عنوان (IP) وبرامج الحماية، وما نسبته (٢٠,٢٪) يرون أنه يمكن تحديده بواسطة عنوان (IP) وبرامج الحماية ووسائل تتبع المخترقين، وما نسبته (٥٣,٨٪) يرون أنه يمكن تحديده بواسطة عنوان (IP) وبرامج الحماية وسائل تتبع المخترقين وبرامج تتبع مصدر الرسائل. وما نسبته (٤,٨٪) يرون أنه يمكن تحديده بواسطة عنوان ((IP وبرامج الحماية وبرامج تتبع مصدر الرسائل. ويشير هذا إلى أن أكثر من نصف عينة الدراسة أنه بالإمكان الاعتماد على الوسائل جميعاً، ويستنتج من هذا أنه بالإمكان الاعتماد عليها حسب النسب التالية (مرتبة حسب أهميتها) عنوان (IP) (٩٤,٢٪)، برامج الحماية (٩١,٤٪)، ووسائل تتبع المخترقين (٧٤,٩٪)، وبرامج تتبع مصدر الرسائل الإلكترونية (٥٩,٦٪).

٢. أفاد ما نسبته (٢٠,٢٪) من عينة الدراسة أنه يمكن تحديد شخصية مرتكب جريمة نظم المعلومات بوسائل أمن البيانات فقط، وما نسبته (١١,٥٪) أفادوا بأنه يمكن تحديده بواسطة تتبع إجراءات أمن العاملين فقط، وما نسبته (٦٨,٣٪) (وهم الأغلب) أفادوا بأنه يمكن تحديده باستخدام وسائل أمن البيانات وتتبع إجراءات أمن العاملين معاً.

ويستنتج مما سبق أن برامج الحماية تعد وسيلة ضبط وتحقيق هامة بشكل دائم، بالإضافة أنها تساعد بما نسبته (٩٤,٢٪) في تحديد نوع الجريمة، وما نسبته (٩٥,١٪) في تحديد توقيت ارتكاب الجريمة، وما نسبته (٧٥٪) في تحديد مصدر الجريمة، وما نسبته (٩٤,٢٪) في الإعلام بوجود جريمة مرتكبة. كما كشفت أنه بالإمكان الاعتماد على الوسائل التالية لتحديد شخصية مرتكب جريمة نظم المعلومات في المؤسسات (وهي مرتبة حسب أهميتها) عنوان (IP) (٩٤,٢٪)، برامج الحماية (٩١,٤٪)، ووسائل تتبع المخترقين (٧٤,٩٪)، وبرامج تتبع مصدر الرسائل الإلكترونية (٥٩,٦٪). وهذا يتفق مع توصيا ت دراسة كل من (البشري، وعبد المطلب) حول أهمية استخدام التقنية بالتحقيق في جرائم نظم المعلومات.

٦-٣-٤-٤ الأدوات المساعدة بالتحقيق

يوضح جدول رقم (٣١) استجابة عينة المحققين بالأجهزة الأمنية والعاملين في مجال نظم المعلومات وموفري تقنيات أمن النظم والبالغ عددهم (١٤١) فرداً حول تقييمهم لمدى أهمية أدوات المساعدة بالتحقيق، وكانت النتائج على النحو التالي:

١. أكدت إجابات عينة الدراسة بدرجة قوية أهمية أداة فك التشفير كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٧٦,٦٪)، مقابل ما نسبته (١٣,٥٪) من الذين اعترضوا على أهميتها، وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٩٥) ويمثل نسبة قدرها (٩,٠٪)، كما يشير الانحراف المعياري والبالغ قدرة (٠,٩٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. أكدت إجابات عينة الدراسة بدرجة قوية أهمية برامج كسر كلمة المرور كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٥١,٧٪)، مقابل ما نسبته (٢,١٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي

Mean (٣,٩٣) ويمثل نسبة قدرها (٧٨,٦٪)، كما يشير الانحراف المعياري والبالغ قدرة (٠,٩٥) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٣. أكدت إجابات عينة الدراسة بدرجة قوية أهمية أدوات استرجاع المعلومات من الأقراص التالفة مثل View disk كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٤٩,٧٪)، مقابل ما نسبته (٢,١٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٩٢) كما يشير الانحراف المعياري والبالغ قدرة (١,٠٠) إلى عدم تقارب تركز إجابات عينة الدراسة وتشتتها.

٤. أكدت إجابات عينة الدراسة بدرجة قوية أهمية برامج مقارنة النسخ كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٦٣,٩٪)، مقابل ما نسبته (٧,١٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٧٨) ويمثل نسبة قدرها (٧٥,٦٪)، كما يشير الانحراف المعياري والبالغ قدرة (٠,٦٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٥. أكدت إجابات عينة الدراسة بدرجة قوية أهمية برامج تشغيل الحاسب مثل Bootable diskette كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٣٢,٦٪)، مقابل ما نسبته (٢,٨٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٢٩) ويمثل نسبة قدرها (٦٥,٨٪)، كما يشير الانحراف المعياري والبالغ قدرة (٠,٥١) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٦. أكدت إجابات عينة الدراسة بدرجة متوسطة أهمية برامج البحث عن الملفات العادية والمخفية مثل Xtreepro gold كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٤١,١٪)، مقابل ما نسبته (٢٠,٥٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب السادس، حيث

بلغت قيمة المتوسط الحسابي Mean (٣,١٨) ويمثل نسبة قدرها (٦٣,٦٪)، كما يشير الانحراف المعياري والبالغ قدرة (٠,٨٠) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٧. أكدت إجابات عينة الدراسة بدرجة قوية متوسطة برامج نسخ البيانات مثل Lap link كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (١٨,٤٪)، مقابل ما نسبته (١٣,٥٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٠٥) كما يشير الانحراف المعياري والبالغ قدرة (٠,٥٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٨. أكدت إجابات عينة الدراسة بدرجة متوسطة أهمية برامج الضغط وفك الضغط Pkzip كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٢٢,٧٪)، مقابل ما نسبته (١٣,٥٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب الثامن، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٠٢) ويمثل نسبة قدرها (٦٠,٤٪)، كما يشير الانحراف المعياري والبالغ قدرة (٠,٧٦) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٩. أكدت إجابات عينة الدراسة بدرجة متوسطة أهمية برامج اتصالات مثل Lantastic كوسيلة مساعدة بالتحقيق، حيث بلغت نسبة الذين وافقوا على أهميتها (٢١,٧٪)، مقابل ما نسبته (٥٣,٦٪) من الذين اعترضوا على أهميتها. وقد حاز على الترتيب التاسع، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٥٢) ويمثل نسبة قدرها (٥٠,٤٪)، كما يشير الانحراف المعياري والبالغ قدرة (٠,٩٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٦-٣-٥ العوائق التي تحول دون استخدام تلك الوسائل

يدخل تحت هذه المعوقات معوق عدم وجود تشريع واضح، ومعوقات متعلقة بالجريمة، ومعوقات متعلقة بالجهة المتضررة من جرائم نظم المعلومات، ومعوقات متعلق بجهات التحقيق.

٦-٣-٥-١ معوق عدم وجود تشريع واضح

يبرز جدول رقم (٣٢) تقييم عينة الدراسة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) والبالغ عددهم (١٤١) فرداً لمدى اعتبارهم لعدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد عائق للتحقيق، إذ أبدو موافقتهم بشدة اتجاه تلك المعوق، حيث بلغت نسبة الموافقين (٩٩,٢٪)، وقد بلغت قيمة المتوسط الحسابي Mean (٤,٦٣). وهذا يشير إلى أن عدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد يعد عائقاً للتحقيق بدرجة كبيرة جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٥٧) إلى تركز الإجابات وعدم تشتتها.

٦-٣-٥-٢ معوقات متعلقة بالجريمة

يوضح جدول رقم (٣٣) استجابة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) والبالغ عددهم (١٤١) فرداً حول تقييمهم للمعوقات التحقيق المتعلقة بالجريمة على النحو التالي:

١. ترى العينة عدم المعرفة بمكونات عناصر جريمة نظم المعلومات من قبل الأطراف المعنية بالجريمة معوقاً للتحقيق بدرجة كبيرة، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٥٦) ويمثل نسبة قدرها (٦٦,٤٪)، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٥٨) إلى تركز الإجابات وعدم تشتتها.

٢. لم ترى العينة إمكانية ارتكاب جرائم نظم المعلومات عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط عائقاً للتحقيق، حيث بلغت قيمة المتوسط الحسابي Mean (١,٩٥) ويمثل نسبة قدرها (٦٦,٤٪). ويشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٧٩) إلى تركز الإجابات وعدم تشتتها.

٦-٣-٥-٣ معوقات متعلقة بالجهة المتضررة من جرائم نظم المعلومات

توضح جداول أرقام (٣٤، ٣٦، ٣٧، ٣٨) على الترتيب استجابة عينة الدراسة (المحققين بالأجهزة الأمنية، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن النظم) حول مدى موافقتهم على اعتبار المعوقات التالية معوقات للتحقيق، حيث جاءت النتائج على النحو التالي (مرتبة حسب حجم ذلك المعوق ما عدا كل من معوق الإحجام عن الإبلاغ لكونه يحتوي على أكثر من متغير، ومعوق التنسيق لكونه متغير نوعي):

١. ترى عينة الدراسة أن متغير معظم المؤسسات المتضررة من جرائم نظم المعلومات لا تتقدم بشكوى للجهات الرسمية معوقاً للتحقيق بدرجة كبيرة جداً، وبلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (٤١,١٪) ونسبة الموافقين (٢٦,٢٪) ولم يعترض على ذلك أحد، وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٩) ويمثل نسبة قدرها (٨١,٨٪). كما يشير الانحراف المعياري والبالغ قدرة (٠,٨٦) إلى تركز الإجابات وعدم تشتتها.

٢. ترى عينة الدراسة أن عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين معوقاً للتحقيق بدرجة كبيرة، إذ بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (١٩,١٪) ونسبة الموافقين (٥١,٨٪)، مقابل نسبة قليلة اعترضت مثلت (٥,٠٪). وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٥) ويمثل نسبة قدرها (٧٧,٠٪). ويشير الانحراف المعياري والبالغ قدرة (٠,٧٨) إلى تركز الإجابات وعدم تشتتها.

٣. ترى عينة الدراسة أن مقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية عائقاً للتحقيق بدرجة كبيرة، إذ بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (١٤,٩٪) ونسبة الموافقين (٥٣,٢٪)، ولم يعترض على ذلك أحد، وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٣) ويمثل نسبة قدرها (٧٦,٦٪). كما يشير الانحراف المعياري والبالغ قدرة (٠,٦٧) إلى تركز الإجابات وعدم تشتتها.

٤. ترى عينة الدراسة أن عدم قناعة العاملين بمجال نظم المعلومات في تدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية عائقاً للتحقيق بدرجة كبيرة، بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (٩,٩٪) ونسبة الموافقين (٣٧,٦٪)، مقابل ما نسبته (٣٠,٥٪) من المعترضين. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٣) ويمثل نسبة قدرها (٧٦,٦٪). كما يشير الانحراف المعياري والبالغ قدرة (١,٣٥) إلى عدم تركز الإجابات وتشتتها.

٥. ترى عينة الدراسة أن عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق عائقاً للتحقيق بدرجة كبيرة، حيث أبدو موافقتهم تجاه تلك المعوق بدرجة كبيرة، إذ بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (٤,٣٪) ونسبة الموافقين (٤٤,٧٪)، مقابل نسبة قليلة اعترضت مثلت (٥,٠٪). وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٤٨) ويمثل نسبة قدرها (٦٩,٦٪). كما يشير الانحراف المعياري والبالغ قدرة (٠,٥٨) إلى تركز الإجابات وعدم تشتتها.

٦. ترى عينة الدراسة أن عدم وجود مردود مادي ملحوظ لتحديث برامج الحماية والتحقيق عائقاً للتحقيق بدرجة متوسطة، إذ بلغت نسبة الموافقين على كونه عائقاً للتحقيق (٥٣,٩٪)، مقابل ما نسبته (٤٤,٠٪) من المعترضين. وقد حاز على الترتيب السادس، حيث بلغت قيمة المتوسط

الحسابي Mean (٣,٠٩) ويمثل نسبة قدرها (٦١,٨٪). كما يشير الانحراف المعياري والبالغ قدرة (٠,٦٧) إلى تركز الإجابات وعدم تشتتها.

٧. ترى عينة الدراسة أن عدم متابعة المستجدات حول جرائم نظم المعلومات عائقاً للتحقيق بدرجة متوسطة، إذ بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (٤,٣٪)، مقابل ما نسبته (١٤,٩٪) من المعترضين. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٩٤) ويمثل نسبة قدرها (٥٨,٨٪). كما يشير الانحراف المعياري والبالغ قدرة (٠,٥٦).

٨. ترى عينة الدراسة أن عدم وجود قسم متخصص في جرائم نظم المعلومات عائقاً للتحقيق بدرجة متوسطة، إذ بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (١٦,٣٪) ونسبة الموافقين (٤,٣٪)، مقابل ما نسبته (٤٨,٢٪) من المعترضين. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٨٩) ويمثل نسبة قدرها (٥٧,٨٪). كما يشير الانحراف المعياري والبالغ قدرة (١,٠٨) إلى تركز الإجابات وعدم تشتتها.

٩. ترى عينة الدراسة أن عدم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات عائقاً للتحقيق بدرجة متوسطة، إذ بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (٢١,٣٪) ونسبة الموافقين (٤,٣٪)، مقابل ما نسبته (٢٤,١٪) من المعترضين. وقد حاز على الترتيب السابع، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٧٥) ويمثل نسبة قدرها (٥٥,٠٪). كما يشير الانحراف المعياري والبالغ قدرة (١,٤٤) إلى عدم تركز الإجابات وتشتتها.

١٠. لا ترى عينة الدراسة أن تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية عائقاً للتحقيق، إذ بلغت نسبة الموافقين بشدة على كونه عائقاً للتحقيق (٢,١٪) ونسبة الموافقين (١١,٣٪)، مقابل ما نسبته (٨٠,١٪) من المعترضين. وقد حاز على الترتيب الأخير، حيث بلغت

قيمة المتوسط الحسابي Mean (٢,١٢) ويمثل نسبة قدرها (٤٤,٢٪). كما يشير الانحراف المعياري والبالغ قدرة (٠,٩٧) إلى تركز الإجابات وعدم تشتتها.

١١. أما عن أسباب الإحجام عن الإبلاغ عن جرائم نظم المعلومات جاءت نتائجها على النحو التالي:

أ. أفاد ما نسبته (٧٦,٠٪) من عينة الدراسة أن حجم الإحجام عن الإبلاغ عن جرائم نظم المعلومات بسبب الحفاظ على السمعة عالي جداً، وما نسبته (٢٤,٠٪) أفادوا بأن حجمه عالي. وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٧٥) ويمثل نسبة قدرها (٤٤,٢٪). وهذا يشير إلى أن حجم الإحجام عن الإبلاغ عنها بسبب الحفاظ على السمعة عالي جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٤٢) إلى تركز الإجابات وعدم تشتتها.

ب. أفاد ما نسبته (٤٥,٢٪) من عينة الدراسة أن حجم الإحجام عن الإبلاغ عن جرائم نظم المعلومات بسبب عدم الرغبة في الظهور بمظهر الضحية عالي جداً، وما نسبته (٤٧,١٪) أفادوا بأن حجمه عالي. وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٣٨) ويمثل نسبة قدرها (٤٤,٢٪). وهذا يشير إلى أن حجم الإحجام عن الإبلاغ عنها بسبب عدم الرغبة في الظهور بمظهر الضحية عالي جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٦٣) إلى تركز الإجابات وعدم تشتتها.

ج. أفاد ما نسبته (٤٣,٣٪) من عينة الدراسة أن حجم الإحجام عن الإبلاغ عن جرائم نظم المعلومات بسبب الخوف من المسؤولية عالي جداً، وما نسبته (٤١,٣٪) أفادوا بأن حجمه عالي. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٢٧) ويمثل نسبة قدرها (٤٤,٢٪). وهذا يشير إلى أن حجم الإحجام عن الإبلاغ عنها بسبب الخوف من المسؤولية

عـالي جـداً، كمـا يشـير الانحـراف المعيـاري Std.Deviation والبـالغ قـدرة (٠,٧١) إلـى تركـز الإجابات وعدم تشتتها.

د. أفـاد مـا نسـبته (٣٢,٧٪) مـن عينـة الدراسـة أن حجـم الإحجـام عـن الإبـلاغ عـن جـرائم نظـم المعلومات بسبب محدودية الآثار المترتبة على الجريمة عالي جداً، وما نسبته (٥٠,٠٪) أفادوا بأن حجمه عالي، مقابل ما نسبته (٢,٩٪) أفادوا بأنه لا يحدث. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٠٩) ويمثل نسبة قدرها (٤٤,٢٪). وهذا يشير إلى أن حجم الإحجام عن الإبلاغ عنها بسبب محدودية الآثار المترتبة على الجريمة عالي جداً، كما يشير الانحراف المعياري ،Std.Deviation والبالغ قدرة (٠,٨٥) إلى تركز الإجابات وعدم تشتتها.

هـ. أفاد ما نسبته (٢٥,٠٪) من عينة الدراسة أن حجم الإحجام عن الإبلاغ عن جرائم نظم المعلومات بسبب عدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع عالي جداً، وما نسبته (٣٤,٦٪) أفادوا بأن حجمه عالي، مقابل ما نسبته (١٩,٢٪) أفادوا بأن حجمه محدود، وما نسبته (١,٩٪) أفادوا بأنه لا يحدث. وقد حاز على الترتيب الخامس، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٦١) ويمثل نسبة قدرها (٤٤,٢٪). وهذا يشير إلى أن حجم الإحجام عن الإبلاغ عنها بسبب عدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع عالي، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,١١) إلى عدم تركز الإجابات وتشتتها.

و. أفـاد مـا نسـبته (٣١,٧٪) مـن عينـة الدراسـة أن حجـم الإحجـام عـن الإبـلاغ عـن جـرائم نظـم المعلومات بسبب عدم إبراز كفاءة المجرمين عالي، مقابل ما نسبته (٢١,٢٪) أفادوا بأن حجمه محدود، وما نسبته (٣٦,٥٪) أفادوا بأن لا يحدث. وقد حاز على الترتيب السادس، حيث بلغت قيمة المتوسط الحسابي Mean (٢,٣٨) ويمثل نسبة قدرها (٤٤,٢٪). وهذا يشير إلى أن حجم

الإحجام عن الإبلاغ عنها بسبب عدم إبراز كفاءة المجرمين محدود، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (١,٢٧) إلى تركز الإجابات وعدم تشتتها.

١٢. أما من ناحية التنسيق بين الأجهزة الأمنية والمؤسسات المستخدمة لنظم المعلومات فتبلغ نسبة الذين ذكروا أن التنسيق متوفر وغير معمول به (٢,٩٪)، مقابل نسبة الذين ذكروا أن التنسيق غير متوفر ولكن ضرورياً (٩٣,٣٪)، وما نسبته (٣,٨٪) ذكروا أنه ليس ضرورياً. وهذا يشير إلى عدم توفر التنسيق بين الأجهزة الأمنية والمؤسسات المستخدمة لنظم المعلومات وعدم العمل به.

١٣. أما من ناحية التنسيق بين المؤسسات المستخدمة لنظم المعلومات والشركات الموفرة لأمن المعلومات، فتبلغ نسبة الذين ذكروا أن التنسيق متوفر ومعمول به (٢١,٢٪)، مقابل ما نسبته (٦٣,١٪) ذكروا أنه متوفر وغير معمول به، وما نسبته (١٢,٥٪) ذكروا أنه غير متوفر ولكن ضرورياً، وما نسبته (٢,٩٪) ذكروا أنه غير متوفر وغير ضروري. وهذا يشير إلى التنسيق بين المؤسسات المستخدمة لنظم المعلومات والشركات الموفرة لأمن المعلومات وغير معمول به.

يتفق هذا مع دراسة (البشري) ومع ما ذكره (الشدي، ١٤٢١هـ) بعدم الإبلاغ عن الجرائم. وأيضاً يتفق مع دراسة (المسند، والمهيني، ١٤٢١هـ)، حيث ذكرا أن أكثر المنشآت تتكتم على ما يحدث لنظمها من اختراقات حيث تشير الإحصائيات إلى أن (١١٪) هو ما يتم الإبلاغ عنه. وكما جاء في دراسة (الشهري) حيث أفادت بأن ما نسبته (٨٩,٤٪) من عينة الدراسة لم يتلقوا بلاغ عن جرائم نظم المعلومات

٤-٥-٣-٦ معوقات متعلق بجهات التحقيق

توضح كل من جداول أرقام (٣٥، ٣٩، ٤٠، ٤١) استجابة عينة الدراسة (المحققين بالأجهزة الأمنية) حول تقييمهم لمدى الموافقة على وجود المعوقات التالية (عدم توفير الكفاءة

البشرية القادرة على التحقيق، عدم توفير الأجهزة والبرامج المناسبة، عدم توفير المتخصصين والخبراء في الحاسب الآلي في جهات التحقيق، عدم التدريب في معاهد متخصصة بالتحقيق في جرائم نظم المعلومات) معوقات للتحقيق، حيث جاءت النتائج على النحو التالي

١. أفادت استجابة عينة الدراسة (المحققين بالأجهزة الأمنية) حيال تقييمهم لعائق عدم توفر الكفاءة البشرية القادرة على التحقيق في جرائم نظم المعلومات، حيث وجد معوق عدم توفر المهارة العالية لاستخدام الحاسب الآلي والإنترنت لدى حوالي نصف العينة (٤٧,٩٪)، كما وجد معوق عدم المعرفة بمتطلبات أمن المعلومات لدى أكثر من ثلثي العينة (٦٦,٧٪)، ومعوق عدم المقدرة على إتباع السياسة الأمنية للتعامل مع الجرائم لدى أكثر من ربع العينة (١٩,٥٪)، كما وجد معوق عدم المعرفة بأساليب ارتكاب جرائم نظم المعلومات لدى أكثر من ثلثي العينة (٧٢,٢٪)، ومعوق عدم المقدرة على الإثبات الجنائي لجرائم نظم المعلومات لدى نصف العينة (٥٢,٢٪).

٢. أفاد ما نسبته (١٣,٩٪) من عينة الدراسة بأن الأجهزة والبرامج المناسبة للتحقيق متوفرة وغير مستخدمة، مقابل ما نسبته (٨٦,١٪) أفادوا بأنها غير متوفرة ولكن توفرها ضروري. وهذا يشير إلى عدم توفر الأجهزة والبرامج المناسبة للتحقيق بجهات التحقيق وعدم استخدامها.

٣. ذكر ما نسبته (١٣,٩٪) من عينة الدراسة بأن المتخصصين والخبراء في الحاسب الآلي متوفرين وتتم الاستفادة منهم، وما نسبته (١٦,٧٪) ذكروا أنهم متوفرين وغير مستفاد منهم، وما نسبته (٦٩,٤٪) ذكروا أنهم غير متوفرين ولكن توفرها ضرورياً. وهذا يشير إلى عدم توفر المتخصصين والخبراء في الحاسب الآلي في جهات التحقيق وعدم الاستفادة منهم.

٤. أفاد ما نسبته (١٣,٩٪) من عينة الدراسة بأن التدريب في معاهد متخصصة بالتحقيق في جرائم نظم المعلومات متوفرة وغير مستخدمة، مقابل ما نسبته (٨٦,١٪) أفادوا بأنها غير متوفرة ولكن

توفرها ضروري. وهذا يشير إلى عدم توفر التدريب في معاهد متخصصة بالتحقيق في جرائم نظم المعلومات وعدم استخدامها.

ويتفق ما سبق مع دراسة (بحر، ١٤٢٠هـ)، حيث ذكر أن المعوقات الشخصية لدى (٦٦,٣٪) من عينة الدراسة. كما تتفق مع دراسة (الشهري، ١٤٢٢هـ)، حيث أظهرت دراسته عدد من المعوقات الإدارية في التعامل الأمني، من أهمها نقص المعرفة بالحاسب الآلي إذ بلغ المتوسط (٤,٦١) ونقص مهارات التعامل مع الإنترنت (٤,٣٩) وعدم كفاية التدريب، وعدم توفير الاتصال بالإنترنت، وعدم توفر أجهزة حاسب، والخبراء، كما يدخل من ضمن تلك المعوقات عدم الإبلاغ عن الجريمة (٣,٥١)، ونقص الأنظمة المجرمة لها (٣,٨٧)، ووضحت دراسته أن هناك فرق ذي دلالة إحصائية بين المؤهل العلمي والمعرفة بالجرائم لصالح المؤهل العلمي العالي. وبعزي الباحث هذا عدم وجود دراسات توضح متطلبات التحقيق ووسائله وإجراءاته، وكذلك عدم وجود جهة يعهد إليها التحقيق

٦-٣-٦ أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات

يوضح جدول رقم (٣٦) استجابة عينة المحققين بالأجهزة الأمنية والبالغ عددهم (٣٦) فرداً حول تقييمهم لمدى أهمية أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات، وكانت النتائج على النحو التالي:

١. يرى ما نسبته (٨٨,٩٪) من عينة الدراسة بأن تسجيل الوقائع كدليل إلكتروني مهم، مقابل ما نسبته (١١,١٪) يرونه غير مهم. وقد حاز على الترتيب الأول، حيث بلغت قيمة المتوسط الحسابي Mean (٤,٥٠)، وهذا يشير إلى أن تسجيل الوقائع كدليل إلكتروني مهم جداً، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٨) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٢. يرى ما نسبته (٨٨,٩٪) من عينة الدراسة بأن التغير الظاهر على البرامج كدليل إلكتروني مهم، مقابل ما نسبته (١١,١٪) يرونه غير مهم. وقد حاز على الترتيب الثاني، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٨٦)، وهذا يشير إلى أن التغير الظاهر على البرامج كدليل إلكتروني مهم، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٥٤) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٣. يرى ما نسبته (٧٥,٠٪) من عينة الدراسة بأن وجود أحصنة طروادة كدليل إلكتروني مهم، مقابل ما نسبته (١٦,٧٪) يرونه غير مهم. وقد حاز على الترتيب الثالث، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٥٦)، وهذا يشير إلى أن وجود أحصنة طروادة كدليل إلكتروني مهم، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٩٤) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

٤. يرى ما نسبته (٦٦,٧٪) من عينة الدراسة بأن وجود فيروسات كدليل إلكتروني مهم، مقابل ما نسبته (١٣,٩٪) يرونه غير مهم. وقد حاز على الترتيب الرابع، حيث بلغت قيمة المتوسط الحسابي Mean (٣,٥٣)، وهذا يشير إلى أن وجود فيروسات كدليل إلكتروني مهم، كما يشير الانحراف المعياري Std.Deviation والبالغ قدرة (٠,٨٤) إلى تقارب وتركز إجابات عينة الدراسة وعدم تشتتها.

ويتضح من السابق أنه بالإمكان الحصول على أدله إلكترونية مثبتة. وهذا يختلف مع دراسة (المسند، والمهيني، ١٤٢١هـ) حيث ذكرا أنه يصعب اكتشاف جرائم الحاسب الآلي لأنه لا يوجد في الغالب شاهد للقضية أو أدلة يمكن استخدامها لتوصل إلى الجاني.

٦-٣-٧ فحص الفرضيات

<u>الفرضية رقم (١)</u>

لا يوجد علاقة جوهرية ذات دلالة إحصائية بين التزام المؤسسة بتحديث برامجها وبين اكتشاف الجرائم التي تتعرض لها.

يوضح جدول رقم (٤٣) قيم معامل ارتباط سبيرمان Correlation Of Coefficient Spearman لتحديد هل هناك علاقات جوهرية بين المتغيرات واتجاه تلك العلاقات، وقد كانت النتائج على النحو التالي:

١. هناك علاقة ارتباط طردية موجبة دالة إحصائياً عند مستوى (٠,٠٥) ٠٥. Significant At The Level بين التحديث وكل من اختراقات البريد الإلكتروني (٠,٣٠٧)، وإرسال أحصنة طروادة (٠,٢٩٩)، وتغيير البيانات بعد إدخالها (٠,٢٦٣)، وتغيير البرامج والإعدادات (٠,١٧٨)، وهذا يعني أن المؤسسة عند قيامها بتحديث برامج حماية معلوماتها قد تكتشف أن هناك جريمة حدثت من تلك الجرائم السابقة.

٢. هناك علاقة ارتباط جوهرية طردية موجبة دالة إحصائياً عند مستوى (٠,٠١) Significant At The Level ٠١. بين التحديث وإرسال وزراعة الفيروسات (٠,٣٣١)، والتحديث والتنصت والسرقة البيانات (٠,٣٠٨). وهذا يعني أن المؤسسة عند قيامها بتحديث برامج حماية معلوماتها قد تكتشف أن هناك جريمة حدثت من تلك الجرائم السابقة.

ويستنتج مما سبق أن المؤسسة عند قيامها بتحديث برامج حماية معلوماتها قد تكتشف أن هناك جريمة حدثت من تلك الجرائم التالية اختراقات البريد الإلكتروني (٠,٣٠٧)، وإرسال أحصنة طروادة (٠,٢٩٩)، وتغيير البيانات بعد إدخالها (٠,٢٦٣)، وتغيير البرامج والإعدادات (٠,١٧٨)، وتغيير البيانات بعد إدخالها (٠,٢٦٣)، التنصت والسرقة البيانات (٠,٣٠٨)، ونسخ البيانات

لاستفادة منها، (٠,٢٨٩)، وإرسال أحصنة طروادة (٠,٢٩٩)، وإغراق البريد الإلكتروني (٠,٤٢٧).ويتفق هذا مع ما توصل إليه (الشدي) في أن إجراء عمليات التحديث والتغيير في الأنظمة (النظم) ومراجعة إعدادات البرامج قد تؤدي إلى اكتشاف جرائم المعلومات حدثت (الشدي ١٤٢١هـ: ٢٠٩). وهذا يرجع أيضاً إلى خصائص تلك الجرائم والتي منها خفاء الجريمة (بحر، ١٤٢٠هـ: ٤٤)، مما يجعل طريقة كشفها يختلف عن طريقة اكتشاف الجرائم التقليدية. ويعزي الباحث هذا أيضاً إلى نوعية تلك الجرائم التي تم تصميم لها برامج خاصة للحماية منها وهذا واضح في كل من إرسال أحصنة طروادة، وإرسال وزراعة الفيروسات

الفرضية رقم (٢)

لا توجد فروق ذات دلالة إحصائية بين متوسط أراء كل من المحققين، والعاملين في مجال نظم المعلومات، وموفري تقنيات أمن نظم المعلومات حول وسائل التحقيق.

أولاً: الأدوات المساعدة بضبط الجريمة

يوضح جدول رقم (٤٤) قيم اختبار التباين الأحادي One- Way ANOVA لفحص الفروق بين المتوسطات، بالإضافة إلى اختبار شفية Scheffe لتحديد لمن يكون الفرق (الحجم الأعلى)، حيث كانت النتائج على الترتيب (مرتبة حسب قيمة (F) الإحصائية والتي تبين حجم الفرق):

١. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية برامج تتبع مصدر الرسائل كأداة مساعدة بضبط الجريمة، وهذا يتضح من قيمة (F=٢٥,٠٧٨)، عند مستوى دلالة (Sig =٠,٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه مهم جداً، وكل من العاملين ويرونه مهم، وموفري تقنيات أمن نظم المعلومات ويرونه مهم جداً، وكان هذا الفرق لصالح المحققين، والفرق الأخر بين العاملين وموفري تقنيات أمن نظم المعلومات وكان لصالح الموفرين.

٢. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية مراجعة قاعدة البيانات كأداة مساعدة بضبط الجريمة، وهذا يتضح من قيمة (F=١٧,٦٧٧)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه مهم جداً، وكل من العاملين ويرونه مهم، وموفري تقنيات أمن نظم المعلومات ويرونه مهم، كما يشير إلى أنه لا يوجد فرق بين متوسط أراء العاملين وموفري تقنيات.

٣. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية برامج تتبع المخترقين كأداة مساعدة بضبط الجريمة، وهذا يتضح من قيمة (F=١١,١٠٤)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه مهم جداً، وكل من العاملين ويرونه مهم جداً، وموفري تقنيات أمن نظم المعلومات ويرونه مهم، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين وموفري تقنيات أمن النظم.

ثالثاً: الأدوات المساعدة بالتحقيق

يوضح جدول رقم (٤٥) قيم اختبار التباين الأحادي One- Way ANOVA لفحص الفروق بين المتوسطات، بالإضافة إلى اختبار شفية Scheffe لتحديد لمن يكون الفرق (الحجم الأعلى)، حيث كانت النتائج على الترتيب (مرتبة حسب قيمة (F) الإحصائية والتي تبين حجم الفرق):

١. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية برامج الاتصالات مثل Lantastic كأداة مساعدة الجريمة بالتحقيق، وهذا يتضح من قيمة (F=١٢٨,٦٤٥)، عند مستوى دلالة (Sig=٠,٠٠٠١).

ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه مهم، وكل من العاملين ويرونه غير مهم، وموفري تقنيات أمن نظم المعلومات ويرونه غير مهم، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه يوجد فرق بين متوسط أراء العاملين وموفري تقنيات أمن النظم، وكان هذا الفرق لصالح الموفرين.

٢. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية برامج مقارنة النسخ وهذا يتضح من قيمة (F= ٤١,٨١٣)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه مهم جداً، وكل من العاملين بالنظم ويرونه مهم، وموفري تقنيات أمن نظم المعلومات ويرونه متوسط الأهمية، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري تقنيات.

٣. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية برامج البحث عن الملفات العادية والمخفية مثل Xtreepro gold، وهذا يتضح من قيمة (F=٣٩,٩٢٧)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه مهم جداً، وكل من العاملين بالنظم ويرونه مهم، وموفري تقنيات أمن نظم المعلومات ويرونه متوسط الأهمية، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري تقنيات

٤. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية أداة فك التشفير، وهذا يتضح من قيمة (F=٢٧,٢٢٧)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين

متوسط أراء المحققين إذ يرونه مهم جداً، وكل من العاملين ويرونه مهم، وموفري تقنيات أمن نظم المعلومات ويرونه مهم، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري تقنيات.

٥. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية أدوات استرجاع المعلومات من الأقراص التالفة مثل View disk، وهذا يتضح من قيمة (F=٢٦,٧٦٩)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه مهم جداً، وكل من العاملين ويرونه غير مهم، وموفري تقنيات أمن نظم المعلومات ويرونه مهم، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري تقنيات.

٦. وجود فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية برامج الضغط وفك الضغط Pkzip، وهذا يتضح من قيمة (F=٤,٠٩٠)، عند مستوى دلالة (Sig=٠,٠١٩). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يرونه متوسط الأهمية، وموفري تقنيات أمن نظم المعلومات ويرونه أيضاً متوسط الأهمية، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وكل من المحققين وموفري تقنيات.

ثالثاً: الوسائل المستخدمة بضبط الجريمة

يتضح في الجدولين رقمي (٤٦) و(٤٧) على الترتيب نتائج اختبار بيرسون كاي تربيع Person Chi-Square Test لفحص الفروق بين المتغيرات (اقتصر هذا على رأي المحققين، والعاملين في مجال نظم المعلومات)، حيث كانت النتائج على نحو التالي:

١. هناك فرق ذي دلالة إحصائية بين أراء المحققين والعاملين في مجال نظم المعلومات حول مدى أهمية برامج الحماية كوسيلة ضبط جريمة نظم المعلومات، وهذا يتضح من مستوى دلالة (Sig=٠,٠٠٠١). كما بينت النسب المئوية أن المحققين يرون أنه بالإمكان الاعتماد على برامج الحماية كوسيلة تستخدم بضبط جريمة نظم المعلومات، وذلك بتحديد نوع الجريمة حيث بلغت نسبتهم (٨٣,٤٪) مقابل ما نسبته (١٠٠,٠٪) من العاملين، والذين يرون أنه يتم الاعتماد عليها بتحديد مصدر الجريمة بلغت نسبتهم (٨٠,٦٪)، مقابل ما نسبته (٦٧,٦٪) من العاملين، وما نسبته (٨٠,٦٪) يرون بأنه يتم الاعتماد عليها بتحديد توقيت ارتكاب الجريمة، مقابل ما نسبته (١٠٠,٠٪) من العاملين، وما نسبته (٨٠,٦٪) يرون بأنه يتم الاعتماد عليها بالإعلام بوجود جريمة مرتكبة، مقابل ما نسبته (٩٢,٦٪) من العاملين.

٢. هناك فرق ذي دلالة إحصائية بين أراء المحققين والعاملين في مجال نظم المعلومات حول الوسائل المستخدمة بتحديد شخصية مرتكب جريمة نظم المعلومات، وهذا يتضح من مستوى دلالة (Sig =٠,٠٠٠١). كما بينت النسب المئوية أن المحققين يرون أنه بالإمكان الاعتماد على عنوان(IP) بتحديد شخصية مرتكب جريمة نظم المعلومات حيث بلغت نسبتهم (٨٠,٧٪)، مقابل ما نسبته (١٠٠,٠٪) من العاملين، والذين يرون تحديده بواسطة برامج الحماية من المحققين بلغت نسبتهم (٦٩,٥٪)، مقابل ما نسبته (١٠٠,٠٪) من العاملين، ونسبة المحققين الذين ذكروا أنه يمكن تحديده بواسطة وسائل تتبع المخترقين بلغت (٢٢,٥٪)، مقابل ما نسبته (٥٨,٨٪) من العاملين، ونسبة المحققين الذين ذكروا أنه يمكن تحديده بواسطة برامج تتبع مصدر الرسائل بلغت (١٩,٥٪)، مقابل ما نسبته (١٣,٢٪) من العاملين.

الفرضية رقم (٢)

لا توجد فروق ذات دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول مدى الموافقة على وجود عوائق استخدام وسائل ضبط الجريمة والتحقيق فيها.

يوضح جدول رقم (٤٨) قيم اختبار التباين الأحادي One- Way ANOVA لفحص الفروق بين المتوسطات، بالإضافة إلى اختبار شفية لتحديد الفرق (الحجم الأعلى) لصالح من يكون، حيث كانت النتائج على الترتيب (مرتبة حسب قيمة (F) الإحصائية والتي تبين حجم الفرق):

١. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق عدم وجود قسم متخصص في جرائم المعلوماتية، وهذا يتضح من قيمة (F=١٧٨,٣٩٨)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين لا يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٢. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق عدم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات، وهذا يتضح من قيمة (F=١٣٦,٦١٨)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين لا يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٣. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين، وهذا يتضح من قيمة (F=٥٨,٥٥٣)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٤. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق، وهذا يتضح من قيمة (F=٤٠,٩١٩)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم والذين يوافقون على وجود ذلك المعوق، وموفري تقنيات أمن نظم المعلومات والذين يوافقون إلى حد ما على وجوده، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٥. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق التكلفة المالية المرتفعة لاستخدام وسائل التحقيق، وهذا يتضح من قيمة (F=٣٢,٥٣٢)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ لا يوافقون على وجود ذلك المعوق، وكل من العاملين بالنظم والذين يوافقون بشدة على وجود ذلك المعوق، وموفري تقنيات أمن نظم المعلومات والذين يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح العاملين بالنظم وموفري تقنيات أمن

نظم المعلومات، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٦. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق عدم قناعة العاملين في مجال نظم المعلومات بتدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية، وهذا يتضح من قيمة (F=٢٠,٤٤٨)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم والذين لا يوافقون على وجود ذلك المعوق، وموفري تقنيات أمن نظم المعلومات والذين يوافقون إلى حد ما على وجوده، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٧. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق إمكانية ارتكاب هذه الجرائم عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط، وهذا يتضح من قيمة (F=١٤,٦٩)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون إلى حد ما على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين لا يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٨. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق مقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية، وهذا يتضح من قيمة (F=٧,٣٧٣)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير

اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

٩. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية، وهذا يتضح من قيمة (F=٦,٨٠٩). عند مستوى دلالة (Sig =٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون إلى حد ما على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين لا يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

١٠. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق عدم التقدم بشكوى للجهات الرسمية من المؤسسات المتضررة من جرائم نظم المعلومات، وهذا يتضح من قيمة (F=٤,٥٤١)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين لا يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح المحققين، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

١١. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق وجود مردود مادي ملحوظ لتحديث برامج

الحماية والتحقيق، وكان هذا الفرق ذي دلالة إحصائية (F=٤,٠٦١)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين إذ يوافقون بشدة على وجود ذلك المعوق، وكل من العاملين بالنظم وموفري تقنيات أمن نظم المعلومات والذين لا يوافقون على وجود ذلك المعوق، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء العاملين بالنظم وموفري التقنيات.

١٢. هناك فرق ذي دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات نحو معوق عدم المعروفة بمكونات عناصر جريمة نظم المعلومات للأطراف المعنية بالجريمة وكان هذا الفرق ذي دلالة إحصائية (F=٣,٢٠٢)، عند مستوى دلالة (Sig=٠,٠٠٠١). ويشير اختبار شفية أن الفرق كان بين متوسط أراء المحققين، والعاملين بالنظم والذين يوافقون على وجود ذلك المعوق، وكان هذا الفرق لصالح العاملين بالنظم، كما يشير اختبار شفية إلى أنه لا يوجد فرق بين متوسط أراء موفري التقنيات وكل من المحققين والعاملين بالنظم.

٤-٦ خلاصة الفصل السادس

تناول هذا الفصل خصائص عينة الدراسة ونتائجها، وقد أظهرت النتائج ارتفاع معدل جرائم نظم المعلومات بعد ظهور الإنترنت، وأن جرائم نظم المعلومات تحدث في المؤسسات التي تمت دراستها بما نسبته (٢٣,٥٪) بشكل يومي على الأقل، كما أظهرت تلك النتائج تعرض (١٢,٨٪) من مؤسسات عينة الدراسة إلى إنذارات بوجود جريمة عن طريق الإنترنت تصل إلى أكثر من (١٠٠٠) إنذار في الأسبوع. كما أن هناك جرائم حجم حدوثها عالٍ كإرسال وزراعة الفيروسات، ونسخ البرامج والاستخدام غير المصرح به للبرامج، والتلاعب بإدخال البيانات، وتغيير البرامج والإعدادات، وإرسال أحصنة طروادة، والاستيلاء على ما سوى المعلومات، وتغيير البيانات بعد

إدخالها، وتدمير الملفات وقواعد البيانات، واختراقات البريد الإلكتروني، كما أظهرت الدراسة أن جرائم نظم المعلومات تسببت بخسائر مادية في عام ٢٠٠١م لما نسبته (٥٧,٤٪) من مؤسسات عينة الدراسة التي تبلغ خسائرها أكثر من (٥٪) من نسبة أجمالي مصروفات المؤسسة. كما بينت النتائج أنه بالإمكان استخدام برامج الحماية بما نسبته (٩٤,٢٪) في تحديد نوع الجريمة، وما نسبته (٩٥,١٪) في تحديد توقيت ارتكاب الجريمة، وما نسبته (٧٥٪) في تحديد مصدر الجريمة، وما نسبته (٩٤,٢٪) في الإعلام بوجود جريمة مرتكبة. كما أظهرت أنه بالإمكان الاعتماد على بعض الوسائل لتحديد شخصية مرتكب جريمة نظم المعلومات في المؤسسات (وهي مرتبة حسب أهميتها) كعنوان (IP) (٩٤,٢٪)، وبرامج الحماية (٩١,٤٪)، ووسائل تتبع المخترقين (٧٤,٩٪)، وبرامج تتبع مصدر الرسائل الإلكترونية (٥٩,٦٪). كما بينت أن هناك معوقات عدة لاستخدام وسائل التحقيق. كما بينت نتائج الدراسة أهمية أنواع الأدلة المادية المثبتة لارتكاب الجرائم كدليل تسجيل الوقائع، ودليل التغير الظاهر على البرامج، ودليل وجود أحصنة طروادة، ودليل وجود فيروسات، كما بينت النتائج مكونات السياسة الأمنية، وبينت أن هناك فروقاً جوهرية بين متغيرات الدراسة.

الفصل السابع/ الخاتمة

٧-١ المقدمة

تناولت هذه الدراسة في فصلها الأول نطاق المشكلة، وفي فصلها الثاني نظم المعلومات. كما تناول فصلها الثالث وسائل التحقيق، وفي فصلها الرابع الدراسات السابقة. أما فصلها الخامس فقد تناول منهج الدراسة وأسلوبها، وأما الفصل السادس فتم فيه استعراض لنتائج الدراسة. وفي هذا الفصل السابع والأخير يتم فيه عرض لخلاصة الدراسة، ووضع التوصيات المنبثقة من نتائجها.

٧-٢ الخلاصة

تهدف هذه الدراسة إلى تحديد وسائل التحقيق في مجال جرائم نظم المعلومات وذلك بالكشف عن الجوانب المختلفة المحيطة بجريمة نظم المعلومات بتحديدها، ومعرفة دوافعها وإبراز أضرارها، وحصر الأساليب والأدوات المستخدمة من قبل مجرمي نظم المعلومات، وعن كيفية الحصول على تلك الأدوات المستخدمة في ارتكاب جرائم نظم من قبل مجرمي نظم المعلومات بالمملكة، والمنافذ المستخدمة من داخل المؤسسة أو من خارجها لارتكابها، وأدوات ضبط الجريمة والتحقيق فيها، وبيان العوائق التي تحول دون استخدام تلك الوسائل، وتحديد أنواع الأدلة المثبتة لارتكاب تلك الجرائم، وتحديد الإجراءات الأمنية سواء كانت فنية أو إدارية لتحقيق أمن نظم المعلومات، ومعرفة أسس صياغة إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات.

يبلغ مجموع عينة الدراسة بشكلها النهائي (١٤١) فرداً، وتتكون من (٣٦) محققاً، ومن (٦٨) عاملاً بمجال نظم المعلومات، ومن (٣٧) متخصصاً في المؤسسات الموفرة لتقنيات أمن نظم المعلومات. وتتكون مؤسسات عينة العاملين بالنظم من الشركات المتخصصة في مجال تقنية المعلومات تمثل (٥٠,٠٪) من مجموع مؤسسات العاملين، والقطاع الحكومي ويمثل(١٦,٢٪)، والقطاع المصرفي ويمثل (١٦,٢٪)، والشركات غير المتخصصة في مجال تقنية المعلومات وتمثل

(١٧,٦٪)، وتوفر ما نسبته (٩٨,٥٪) من تلك المؤسسات الإنترنت لموظفيها، كما يرتبط (٨٦,٨٪) منها بالإنترنت عن طريق الشبكة المحلية المربوطة بمزود الخدمة، وما نسبته (٧٩,٤٪) منها يوجد بها سياسات أمنية، وما نسبته (٥١,٥٪) منها تصرف أكثر من (٣٠٪) على تقنية المعلومات من أجمالي ميزانيتها، وما نسبته (٤٥,٦٪) منها تمتلك أكثر من (١٠٠٠) جهاز حاسب الآلي، وما نسبته (٧٣,٥٪) منها يتوفر بها قسم متخصص في أمن المعلومات.

تم استخدام أداة الدراسة (الإستبانة) لجمع البيانات اللازمة للدراسة وتكونت من البيانات العامة التي تناولت خصائص عينة الدراسة وتكونت من (٩) فقرات، أما البيانات التفصيلية فشملت مكونات السياسة الأمنية الشاملة لحماية نظم المعلومات وتكونت من (١٢) فقرة الإجراءات الفنية ولإدارية لأمن نظم المعلومات وتكونت من (٣٢) فقرة، وجرائم نظم المعلومات وتكونت من (٨١) فقرة، ووسائل التحقيق في جرائم نظم المعلومات وتكونت من (٣٤) فقرة، والعوائق التي تحول دون استخدام تلك الوسائل وتكونت من (٢٢) فقرة، وأنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات وتكونت من (٤) فقرة. أما النتائج يمكن تلخيصها على النحو التالي:

١. في مجال السياسة الأمنية

أ. قلة إتباع العناصر المتعلقة بالسياسة الأمنية الشاملة بالمؤسسات وهي على الترتيب؛ عدم وجود سياسة أمنية واضحة لأمن نظم المعلومات بالمؤسسات (٤,٩٦)، وعدم اللزام الموظفين بالسياسة الأمنية ووضع عقوبات للمخالفين (٤,٩٣)، وعدم وجود سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية (٤,٩١)، وعدم الإعلان عن السياسة الأمنية للموظفين بما يكفل تبليغها للعموم (٤,٨٠)، وعدم تقيد الرؤساء بالسياسة الأمنية عند إعطاء التعليمات (٤,٤١).

ب. إن أقل العناصر وضوحاً في مكونات السياسة الأمنية الشاملة بالمؤسسات على الترتيب الاحترازات الشخصية (٢٢,٧٪)، والتشارك في الخدمات (٢٢,٧٪)، والعلاقة بالمنافسين

والشركاء (٢٤,١٪)، والوثائق ووسائط الحفظ (٢٧,٠٪)، والبرامج المطورة داخلياً (٢٩,١٪)، والجانب البشري (٤٣,٣٪).

٢. في مجال أمن نظم المعلومات

أ. يدرك أفراد عينة الدراسة (العاملين بمجال نظم المعلومات) بدرجة قوية أهمية وجود إجراءات إدارية وفنية لأمن نظم المعلومات (٤,٩٣).

ب. إن أقل إجراءات التوعية إتباعاً إقامة الندوات والمحاضرات (١٨,١٪)، ثم الاشتراكات بالمجلات والدوريات بلغت نسبتهم (٣٥,٣٪).

ج. إن أقل الإجراءات إتباعاً (على الترتيب) توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها (٢,٢٠)، ومنح الحوافز للالتزام بالإجراءات الأمنية (٢,٢٥)، والتأكد من مزامنة ساعات الأجهزة باستمرار (٢,٤٤)، وربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات (٢,٦٦)، وتحديد مدة صلاحية كلمات المرور وتغييرها (٢,٧٥)، والتقدم بشكوى حول جرائم نظم المعلومات (٢,٩٥)، وتحديث النسخ الاحتياطي المركزي (٣,٠٧). وهذا يدل على أن هناك قصور أمني بإتباع تلك الإجراءات.

د. اختلاف الإجراءات الأمنية المتبعة بالمؤسسات، ويعزى إلى نوع المؤسسات المشمولة بهذه الدراسة إذ يعتمد مستوى الأمن لديها على درجة أهمية معلوماتها والنشاط الذي تمارسه تلك المؤسسات.

٣. جرائم نظم المعلومات

أ. يدرك أفراد عينة الدراسة (المحققين، العاملين بمجال نظم المعلومات) بدرجة قوية خطورة جرائم نظم المعلومات (٤,٥٨).

ب. ارتفاع معدل جرائم نظم المعلومات بعد ظهور الإنترنت (٤,٤٨).

ج. هناك جرائم نظم المعلومات حجم حدوثها عالي وهي على الترتيب؛ إرسال وزراعة الفيروسات (٤,٠٦)، ونسخ البرامج والاستخدام غير المصرح به (٣,٨٩)، والتلاعب بإدخال البيانات (٣,٨٨)، وتغيير البرامج والإعدادات (٣,٨٦)، وإرسال أحصنة طروادة (٣,٨٣)، والاستيلاء على ما سوى المعلومات (٣,٤٠)، وتغيير البيانات بعد إدخالها (٣,٣٢)، وتدمير الملفات وقواعد البيانات (٣,٢٦).

د. هناك أساليب حجم استخدامها عالي نحو المؤسسات (سواء من الداخل المؤسسة أو خارجها)، وهي على الترتيب؛ إرسال الفيروسات بالبريد الإلكتروني أو برامج المحادثة وما شابهها (٤,٥٢)، إرفاق أحصنة طروادة بالبرامج (٤,٢١)، والنفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثور على ملفات مشاركة غير محمية (٣,٨٧)، واستغلال الثغرات التي تكتشف في نظم التشغيل والتطبيقات العاملة معه (٣,٧٤)، ومحاولة اكتشاف المنافذ المفتوحة والدخول منها (٣,٧٤)، IP Spoofing (٣,٦٥)، واستغلال الثغرات الأمنية في مزودات web مثل مزود IIS (٣,٥٩)، واستخدام برامج حديثة تقوم باستغلال نقاط الضعف في برامج الحماية واستغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة (٣,٥٠). واستغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة (٣,٤٧).

هـ. حجم استخدام منفذ شبكة الإنترنت وبرامج الاختراق الموجودة بها (٤,٢٥) كمنفذ خارجي أعلى من المنافذ الداخلية والخارجية الأخرى كإفشاء الرقم السري من قبل الموظفين (٤,١٦)، أو المحاولة المتكررة (٣,٩٥)، أو عن طريق الأجهزة ومحركات الأقراص المرنة والليزر (٣,٩٥)، أو عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد (٣,٩١)، أو الشبكة الواسعة WAN والبرامج المرتبطة (٣,٨٨).

و. هناك أدوات حجم استخدامها عالي نحو المؤسسات (سواء من الداخل المؤسسة أو خارجها)، وهي على الترتيب؛ الفيروسات وديدان الإنترنت (٤,٥٣)، وCookies (٤,٥١)، والبريد

الإلكتروني (٤,١٨)، والمشاركة في الملفات على الشبكة (٤,٠٨)، برامج التنصت على الشبكات (٣,٨٩)، برنامج Net Bus (٣,٨٠)، وبرنامج Sub Seven (٣,٧٥)، وبرنامج ICQ (٣,٥١)، وبرنامج Password Recovery Toolkit (٣,٤٦)، وبرنامج Tribe Flood Network (٣,٢٩).

ز. هناك طرق حجم سلوكها للحصول على أدوات ارتكاب الجرائم عالي، وهي؛ الحصول عليها كبرامج مجانية من مواقع على شبكة الإنترنت (٤,٩٦)، الحصول عليها من أماكن البيع غير قانونية للبرامج (٤,٧١)، الحصول عليها كبرامج غير مجانية تشترى من مواقع على شبكة الإنترنت (٣,٦٦).

ح. تحدث جرائم نظم المعلومات بمؤسسات عيينة الدراسة بشكل يومي على الأقل بما نسبته (٢٣,٥٪) منها، كما تحدث جرائم نظم المعلومات بشكل غير منتظم على الأقل بما نسبته (٤٧,١٪) من مؤسسات عيينة الدراسة

ط. تتعرض ما نسبته (١٥,٩٪) من مؤسسات عيينة الدراسة إلى إنذارات بوجود جريمة عن طريق الإنترنت تصل من (١٠٠) إلى أقل من (١٠٠٠) إنذار في الأسبوع، كما تتعرض ما نسبته (١٢,٨٪) من مؤسسات عيينة الدراسة إلى إنذارات بوجود جريمة عن طريق الإنترنت تصل إلى أكثر من (١٠٠٠) إنذار في الأسبوع.

ي. هناك جهد كبير يبذل لمتابعة جرائم نظم المعلومات من قبل قسم خاص بالمؤسسات (٣,٩٦).

ك. هناك اعتماد كبير على ضمانات موردي الأجهزة والبرامج بدلاً من تتبع الجرائم (٣,٣٨).

ل. تسببت جرائم نظم المعلومات لما نسبته (٤٢,٦٪) من مؤسسات عينة الدراسة بخسائر مادية لما نسبته (٣٦,٨٪) من مؤسسات عينة الدراسة بخسائر مادية تبلغ من (٥٪) إلى أقل من (١٠٪) من نسبة أجمالي مصروفات المؤسسة. وتسببت لما نسبته (٢٠,٦٪) من مؤسسات عينة

الدراسة بخسائر مادية تبلغ أكثر من (١٠٪) من نسبة أجمالي مصروفات المؤسسة في عام ٢٠٠١م.

م. ارتفاع حجم بعض دوافع جرائم نظم المعلومات، وهي على الترتيب دافع التسلية وحب الاستطلاع (٤,١٩)، ودافع الوصول إلى معلومات شخصية (٤,٠٦)، ودافع إبراز القدرات (٤,٠٢)، ودافع الانتقام (٣,٩٨)، ودافع الاقتصادي والتجاري (٣,٢٥).

٤. وسائل التحقيق في جرائم نظم المعلومات

أ. أنه بالإمكان استخدام تقنية المعلومات بشكل دائم كوسيلة من وسائل ضبط الجريمة والتحقيق، كما تعد برامج الحماية وسيلة ضبط وتحقيق هامة بشكل دائم، بالإضافة أنها تساعد بما نسبته في تحديد نوع الجريمة (٩٤,٢٪) وتحديد توقيت ارتكاب الجريمة (٩٥,١٪) وتحديد مصدر الجريمة (٧٥٪)، والإعلام بوجود جريمة مرتكبة (٩٤,٢٪).

ب. أنه بالإمكان الاعتماد على الوسائل التالية لتحديد شخصية مرتكب جريمة نظم المعلومات في المؤسسات (وهي مرتبة حسب أهميتها) عنوان (IP) (٩٤,٢٪)، برامج الحماية (٩١,٤٪)، ووسائل تتبع المخترقين (٧٤,٩٪)، وبرامج تتبع مصدر الرسائل الإلكترونية (٥٩,٦٪).

ج. أنه بالإمكان الاعتماد على الوسائل التالية لتحديد شخصية مرتكب جريمة نظم المعلومات في المؤسسات (وهي مرتبة حسب أهميتها) عنوان (IP) (٩٤,٢٪)، برامج الحماية (٩١,٤٪)، ووسائل تتبع المخترقين (٧٤,٩٪)، وبرامج تتبع مصدر الرسائل الإلكترونية (٥٩,٦٪). ووسائل أمن البيانات (٨٨,٥٪)، وتعقب إجراءات أمن العاملين (٧٩,٨٪)

د. أهمية الأدوات التالية والمساعدة بالضبط الجريمة (مرتبة حسب أهميتها) سجل الصلاحيات للمستخدمين (٤,٩٤)، والتقارير التي تنتجها نظم أمن البيانات (٤,٨٦)، وبرامج النسخ الاحتياطي والتسجيل Logging (٤,٧٦)، وبرامج كشف الفيروسات (٤,٧٤)، وأدوات

المراجعة Auditing (٤,٦٩)، وتقارير الجدران النارية (٤,٥٣)، وأدوات مراقبة المستخدمين للشبكة (٤,٥٢)، وبرامج تتبع المخترقين (٤,١١)، ومراجعة قاعدة البيانات (٤,٠٧)، برامج تتبع مصدر الرسائل (٤,٠٦).

هـ. أهمية الأدوات التالية والمساعدة بالتحقيق (مرتبة حسب أهميتها) أداة فك التشفير (٣,٩٥)، وبرامج كسر كلمة المرور (٣,٩٣)، وأدوات استرجاع المعلومات من الأقراص التالفة مثل View disk (٣,٩٢)، وبرامج مقارنة النسخ (٣,٧٨)، وبرامج تشغيل الحاسب مثل Bootable diskette (٣,٢٩).

و. أهمية أنواع الأدلة الإلكترونية المثبتة لارتكاب جرائم نظم المعلومات التالية، (مرتبة حسب أهميتها) تسجيل الوقائع (٤,٥٠)، والتغير الظاهر على البرامج (٣,٨٦)، ووجود أحصنة طروادة (٣,٥٦)، ووجود فيروسات (٣,٥٣).

ز. وجود فرق ذات دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول أهمية أدوات ضبط الجريمة والتحقيق فيها. وهي على الترتيب؛ برامج مقارنة النسخ (F= ٤١,٨١٣)، وبرامج البحث عن الملفات العادية والمخفية مثل Xtreepro gold (F=٣٩,٩٢٧)، وأداة فك التشفير (F=٢٧,٢٢٧)، وأدوات استرجاع المعلومات من الأقراص التالفة مثل View disk (F=٢٦,٧٦٩)، وبرامج تتبع مصدر الرسائل (F=٢٥,٠٧٨)، ومراجعة قاعدة البيانات (F=١٧,٦٧٧)، وسجل الصلاحيات للمستخدمين (F=٩,٧٥٠).

ح. هناك فرق ذي دلالة إحصائية بين أراء المحققين والعاملين في مجال نظم المعلومات حول مدى أهمية برامج الحماية كوسيلة ضبط جريمة نظم المعلومات، حيث أن المحققين يرون أنه بالإمكان الاعتماد على برامج الحماية كوسيلة تستخدم بضبط جريمة نظم المعلومات، وذلك بتحديد نوع الجريمة بنسبة (٨٣,٤٪) مقابل (١٠٠,٠٪) من العاملين، ويرون أنه يمكن الاعتماد

عليها بتحديد مصدر الجريمة بنسبة (٨٠,٦٪)، مقابل (٦٧,٦٪) من العاملين، كما يرون بأنه يتم الاعتماد عليها بتحديد توقيت ارتكاب الجريمة بنسبة (٨٠,٦٪) مقابل (١٠٠,٠٪) من العاملين، ويرون بأنه يتم الاعتماد عليها بالإعلام بوجود جريمة مرتكبة بنسبة (٨٠,٦٪) مقابل (٩٢,٦٪) من العاملين.

ط. هناك فروق ذات دلالة إحصائية بين أراء المحققين والعاملين في مجال نظم المعلومات حول الوسائل المستخدمة بتحديد شخصية مرتكب جريمة نظم المعلومات، حيث يرى المحققين أنه بالإمكان الاعتماد على عنوان (IP) بتحديد شخصية مرتكب جريمة نظم المعلومات بنسبة (٨٠,٧٪)، مقابل ما نسبته (١٠٠,٠٪) من العاملين، والذين يرون تحديده بواسطة برامج الحماية من المحققين بلغت نسبتهم (٦٩,٥٪)، مقابل ما نسبته (١٠٠,٠٪) من العاملين، ونسبة المحققين الذين ذكروا أنه يمكن تحديده بواسطة وسائل تتبع المخترقين بلغت (٢٢,٥٪)، مقابل ما نسبته (٥٨,٨٪) من العاملين، ونسبة المحققين الذين ذكروا أنه يمكن تحديده بواسطة برامج تتبع مصدر الرسائل بلغت (١٩,٥٪)، مقابل ما نسبته (١٣,٢٪) من العاملين.

٥. معوقات استخدام وسائل التحقيق في جرائم نظم المعلومات

أ.ترى عينة الدراسة أن هناك معوقات عدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد (٤,٦٣)، ومعوقات متعلقة بالجريمة هو عدم المعرفة بمكونات عناصر جريمة نظم المعلومات من قبل الأطراف المعنية بالجريمة (٣,٥٦)، ومعوقا ت تتعلق بالجهات المتضررة من جرائم نظم المعلومات، وتشمل؛ عدم تقدم معظم المؤسسات المتضررة من جرائم نظم المعلومات بشكوى للجهات الرسمية (٤,٠٩)، وعدم التدريب على استخدام التقنية المساعدة في كشف المجرمين (٣,٨٥)، ومقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية (٣,٨٣)، وعدم قناعة العاملين بمجال نظم المعلومات في تدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية (٣,٨٣)، وعدم استخدام أدوات تقنية متطورة تناسب

برامج وأدوات التحقيق (٣,٤٨)، وعدم التنسيق بين الأجهزة الأمنية والمؤسسات المستخدمة لنظم المعلومات (٩٣,٣٪). أما معوق الإحجام عن الإبلاغ عن جرائم نظم المعلومات فهي بسبب الحفاظ على السمعة (٤,٧٥)، وبسبب عدم الرغبة في الظهور بمظهر الضحية (٤,٣٨)، وبسبب الخوف من المسؤولية (٤,٢٧)، وبسبب محدودية الآثار المترتبة على الجريمة (٤,٠٩)، بسبب عدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع (٣,٦١)، أما المعوقات المتعلقة بجهات التحقيق فهي؛ عدم توفير الأجهزة والبرامج المناسبة للتحقيق (٨٦,١٪)، وعدم توفير المتخصصين والخبراء في الحاسب الآلي (٦٩,٤٪) وعدم التدريب في معاهد متخصصة بالتحقيق في جرائم نظم المعلومات (٨٦,١٪)، أما معوق عدم توفر الكفاءة البشرية القادرة على التحقيق في جرائم نظم المعلومات فيشمل عدم توفر المهارة العالية لاستخدام الحاسب الآلي والإنترنت لدى حوالي نصف العينة (٤٧,٩٪)، ومعوق عدم المعرفة بمتطلبات أمن المعلومات لدى أكثر من ثلثي العينة (٦٦,٧٪)، ومعوق عدم المقدرة على إتباع السياسة الأمنية للتعامل مع الجرائم لدى أكثر من ربع العينة (١٩,٥٪)، و معوق عدم المعرفة بأساليب ارتكاب جرائم نظم المعلومات لدى أكثر من ثلثي العينة (٧٢,٢٪)، ومعوق عدم المقدرة على الإثبات الجنائي لجرائم نظم المعلومات لدى أكثر من نصف العينة (٥٢,٢٪).

ب. وجود فرق ذات دلالة إحصائية بين متوسط أراء المحققين والعاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات حول مدى الموافقة على عوائق التحقيق. حيث أن متوسط موافقة المحققين أكبر من العاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات إزاء المعوقات وهي على الترتيب (حسب قيمة (F) الإحصائية) معوق عدم وجود قسم متخصص في جرائم المعلوماتية (F=١٧٨,٣٩٨)، وعدم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات (F=١٣٦,٦١٨)، ومعوق عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين (F=٥٨,٥٥٣)، ومعوق عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق (F=٤٠,٩١٩)، ومعوق التكلفة المالية المرتفعة لاستخدام وسائل

التحقيق (F=٣٢,٥٣٢)، ومعوق عدم قناعة العاملين في مجال نظم المعلومات بتدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية (F=٢٠,٤٤٨)، ومعوق إمكانية ارتكاب هذه الجرائم عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط (F=١٤,٦٩١)، ومعوق مقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية (F=٧,٣٧٣)، ومعوق تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية(F=٦,٨٠٩).

ج. وجود فرق ذي دلالة إحصائية بين متوسط أراء العينة حيث أن متوسط موافقة المحققين أكبر من العاملين في مجال نظم المعلومات وموفري تقنيات أمن نظم المعلومات إزاء معوق عدم التقدم بشكوى للجهات الرسمية من قبل المؤسسات المتضررة من جرائم نظم المعلومات (F=٤,٥٤١).

٧-٣ التوصيات

٧-٣-١ توصيات متعلقة بأمن نظم المعلومات والسياسات الأمنية

١. أظهرت النتائج أن أقل الإجراءات إتباعاً على الترتيب توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها، ومنح الحوافز للالتزام بالإجراءات الأمنية، والتأكد من مزامنة ساعات الأجهزة باستمرار، وربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات، وتحديد مدة صلاحية كلمات المرور وتغييرها، والتقدم بشكوى حول جرائم نظم المعلومات، وتحديث النسخ الاحتياطي المركزي، مما يدل على أن هناك قصور أمني بإتباع تلك الإجراءات، ولهذا توصي هذه الدراسة بضرورة الاهتمام بإتباعها وبالتالي النهوض بمستوى أمن نظم المعلومات.

٢. أشارت النتائج أن أقل إجراءات التوعية إتباعاً على الترتيب الندوات، والاشتراكات بالمجلات والدوريات التي تعنى بأمن المعلومات، ولهذا توصي هذه الدراسة ضرورة قيام المؤسسات بإقامة الندوات والاشتراك بتلك النوع من المجلات, للتعرف على احدث الطرق والإجراءات التي من شانها أن تساعد على تحقيق أمن المعلومات.

٣. أظهرت النتائج عدم وجود سياسة أمنية واضحة لأمن نظم المعلومات بالمؤسسات، ولهذا توصي هذه الدراسة بضرورة أيجاد سياسة أمنية واضحة للنهوض بمستوى أمن نظم المعلومات.

٤. أظهرت النتائج أهم العناصر التي يجب توفرها بالسياسة الأمنية على الترتيب وجود سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية، اللزام الموظفين بالسياسة الأمنية ووضع عقوبات للمخالفين، إعلان السياسة الأمنية للموظفين بما يكفل تبليغها للعموم، تقيد الرؤساء بالسياسة الأمنية عند إعطاء التعليمات، ولهذا توصي هذه الدراسة بضرورة الاهتمام بتوفير تلك العناصر بالسياسة الأمنية للنهوض بمستوى أمن نظم المعلومات..

٥. أظهرت النتائج أقل العناصر وضوحاً في مكونات السياسة الأمنية الشاملة بالمؤسسات على الترتيب؛ الجانب البشري، البرامج المطورة داخلياً، الوثائق ووسائط الحفظ، استخدام الإنترنت، الاحترازات الشخصية، التشارك في الخدمات، البرامج الجاهزة، العلاقة بالمنافسين والشركاء، ولهذا توصي هذه الدراسة بضرورة الاهتمام بتوضيح تلك العناصر بالسياسة الأمنية للنهوض بمستوى أمن نظم المعلومات.

٧.٣.٢ توصيات متعلقة بالتحقيق

١. أظهرت النتائج أنه بالإمكان استخدام برامج الحماية كوسيلة ضبط للجريمة، حيث أنها تساعد بشكل كبير جداً في تحديد نوع الجريمة، وتوقيت ارتكابها، وتحديد مصدرها، والإعلام بوجود

جريمة مرتكبة، ولهذا توصي هذه الدراسة بضرورة اعتمادها كأداة ضبط للجريمة وذلك للنهوض بمستوى التحقيق بجرائم نظم المعلومات.

٢. أظهرت النتائج أنه بالإمكان الاعتماد على الوسائل التالية لتحديد شخصية مرتكب جريمة نظم المعلومات (وهي مرتبة حسب أهميتها) عناوين (IP، وMAC)، برامج الحماية، ووسائل تتبع المخترقين، وبرامج تتبع مصدر الرسائل الإلكترونية، ولهذا توصي هذه الدراسة بضرورة اعتمادها كأداة تحديد لشخصية مرتكب جريمة نظم المعلومات، وذلك للنهوض بمستوى التحقيق بجرائم نظم المعلومات.

٣. أظهرت النتائج الأهمية القصوى للأدوات التالية والمساعدة بالضبط الجريمة (مرتبة حسب أهميتها) سجل الصلاحيات للمستخدمين، التقارير التي تنتجها نظم أمن البيانات، برامج النسخ الاحتياطي والتسجيل Logging، وبرامج كشف الفيروسات، وأدوات المراجعة Auditing، وتقارير الجدران النارية، وأدوات مراقبة المستخدمين للشبكة، وأدوات التنصت على الشبكة، وبرامج تتبع المخترقين، مراجعة قاعدة البيانات، وبرامج تتبع مصدر الرسائل، ولهذا توصي هذه الدراسة بضرورة اعتمادها كأدوات مساعدة بالضبط الجريمة، وذلك للنهوض بمستوى التحقيق بجرائم نظم المعلومات.

٤. أظهرت إجابات عينة الدراسة أهمية الأدوات التالية والمساعدة بالتحقيق (مرتبة حسب أهميتها) أداة فك التشفير، برامج كسر كلمة المرور كما أدوات استرجاع المعلومات من الأقراص التالفة مثل View disk، وبرامج مقارنة النسخ، وبرامج تشغيل الحاسب مثل Bootable diskette، ولهذا توصي هذه الدراسة بضرورة اعتمادها كأدوات مساعدة بالتحقيق، وذلك للنهوض بمستوى التحقيق بجرائم نظم المعلومات.

٥. كشفت إجابات عينة الدراسة الأهمية القصوى لأنواع الأدلة المادية المثبتة لارتكاب جرائم نظم المعلومات التالية (مرتبة حسب أهميتها) دليل تسجيل الوقائع، دليل التغير الظاهر على البرامج، دليل وجود أحصنة طروادة، دليل وجود فيروسات ولهذا توصي هذه الدراسة بضرورة الاعتماد عليها كأدلة مادية مثبتة لارتكاب الجرائم، وذلك للنهوض بمستوى التحقيق بجرائم نظم المعلومات.

٧-٣-٣ توصيات متعلقة بمعوقات التحقيق

١. أشارت إجابات عينة الدراسة أن هناك معوق للتحقيق هو عدم وجود تشريعات واضحة وخاصة لجرائم نظم المعلومات، بالرغم من أن هناك محاولة لتشريع وسن قوانين في مجال جرائم نظم المعلومات على الصعيد العالمي ومن ضمنه المملكة التي شكلت لجان مكونة من عدة جهات، لإظهار قوانين تحد من جرائم نظم المعلومات، بما في ذلك الجرائم التي ترتكب عن طريق الشبكات، ووضع الضوابط لاستخدام الحكومة والتجارة الإلكترونية، وإيجاد ضوابط استخدام الإنترنت في المملكة والتي أُعدت من قبل لجنة الإنترنت الأمنية الدائمة، والتي ترأسها وزارة الداخلية وبعضوية عدد من الجهات الحكومية. ولهذا توصي هذه الدراسة بضرورة أن تكون هناك نصوصاً واضحةً تمنح الصلاحيات لرجال تحقيق العدالة، بضبط تلك الجرائم وتقديم مرتكبيها للمحاكمة. وذلك للنهوض بمستوى التحقيق بجرائم نظم المعلومات.

٢. التنسيق فيما بين وزارة الداخلية ممثلة بإدارة الشئون الفنية، وجهات التحقيق، والشرطة الدولية والعربية، والمؤسسات المستخدمة للنظم والشركات الموفرة لأمن المعلومات، والشركات المزودة لخطوط الاتصالات، ومزودي خدمة الإنترنت ومدينة الملك عبد العزيز للعلوم والتقنية الجهة المشرفة علي مزودي خدمة الإنترنت والمزود الرئيسي، والقطاعات المصرفية وإدارة التقنية البنكية بمؤسسة النقد الجهة المشرفة على المصارف المالية، والمشاريع المنبثقة من الجهات الحكومية حول بناء حكومة إلكترونية، وتجارة إلكترونية، أو شركات أمن المعلومات، وكليات

الحاسب الآلي في الجامعات، سواء بطريقة مباشرة أو غير مباشرة كل فيما يخصه لمساعدة الجهات الأمنية في ضبط تلك الجرائم وتقديم مرتكبيها للمحاكمة، ويتركز التنسيق على:

أ. نوعية التطبيقات والأجهزة المستخدمة.

ب. أسلوب تقديم خدمة الإنترنت كالاشتراك المباشر، أو البطاقات التي يجب أن تكفل معرفة صاحب البطاقة مع مراعاة حقوق المؤسسات في مجال سهولة وزيادة مبيعاتها، وحقوق المواطن.

ج. من طرق كشف المخترق معرفة (IP) وفي الغالب يكون متغير مما يحتاج إلى تنسيق بين الجهة المتضررة أو الجهة الأمنية ومزودي خطوط الاتصال لمعرفة من أين يتصل.

د. يفيد التنسيق الجهات الغير متضررة من الجرائم بتضمين سياستها الأمنية الحماية من الجرائم التي حصلت لجهات قد تضررت من الجرائم.

٣. تحديد إطار للجهات الأخرى من قبل الجهة الأمنية لكيفية الانسجام مع المتطلبات الأمنية اللازمة لأعمال التحقيق، وتحديد مساهمة كل جهة في تسهيل أعمال التحقيق.

٤. يحتفظون مزودي الخدمة ISP,s في خوادمهم Servers بمعلومات تمكن جهات التحقيق من الاستفادة منها كآثار، وأدلة يجب المحافظة عليها حتى انتهاء عملية التحقيق.

٥. تشكيل قسم خاص لتحقيق في جرائم نظام المعلومات ذو كفاءة عالية، يتكون من المحقق الرئيسي، وفريق استجواب، وفريق تصوير ورسم، وفريق تفتيش، وفريق جمع الأدلة.

٦. قد يعمد المجرم بنقل المعلومات الحساسة عن طريق الشبكة، مما يتطلب إنشأ مركز أمن معلومات تحت مظلة وزارة الداخلية، يكون متخصص بالتحقيق بجرائم نظم المعلومات، ويتكون من فريق ذو مهارة عالية باستخدام الحاسب الآلي والإنترنت، ويكون قادراً على معرفة متطلبات الإثبات

الجنائي لجرائم نظام المعلومات، كما يقوم المركز بإتباع جميع الوسائل لجمع الأدلة الإلكترونية سواء من بريداً إلكترونياً أو سجل لغرف المحادثة أو عن طريق تتبع الأثر للجهاز الذي تم استخدامه للقيام بعملية الاختراق، أو تتبع مصدر الرسائل الإلكترونية، أو مراقبة المستخدمين للشبكة أو المواقع الخاصة بالمخترقين أو المنتديات.

٧. التعاون مع جهات متخصصة وذات خبرة في مجال التحقيق بجرائم الحاسب الآلي والإنترنت لتقوم بتقديم مساعدتها للجهات الأمنية في مجال التحقيق بجرائم نظام المعلومات، كتقديم التقارير عن الجرائم التي تتبعها، والمعلومات الإحصائية عن تلك الجرائم، والمساعدة في تحديث للوائح والتشريعات، وتدريب العاملين في الجهات الأمنية لمكافحة الجرائم، وعقد المؤتمرات، كتلك الجهات التي تساعد FBI مثل The Florida Association of Computer Crime Investigators (FACCI) (FACCI, ٢٠٠٢) أو CERT* advisories and other security information أو (CSI Computer Security Institute).

٨. التدريب في معاهد متخصصة بالتحقيق في جرائم نظام المعلومات، مثل معهد أمن الحاسب الآلي (Computer Security Institute) الذي يقوم بتدريب FBI بالإضافة إلى إعداد التقارير الأمنية. ولهذا يجب العمل على إنشاء أو التعاون مع معاهد تقوم بإعداد فريق تحقيق ذو مهارة عالية لاستخدام الحاسب الآلي والإنترنت ليكون قادراً على معرفة متطلبات أمن المعلومات، ومعرفة أساليب ارتكاب جرائم نظام المعلومات وأدوات ارتكابها، ولإثبات الجنائي لجرائم نظام المعلومات.

٩. توفير الأجهزة والبرامج المناسبة للجهات الأمنية للقيام بمهام التحقيق في مجال جرائم نظم المعلومات.

٤.٧ خلاصة الفصل السابع

تم في هذا الفصل تلخيص فصول الدراسة الستة السابقة، وتفسير نتائج الدراسة، ورصد أهم التوصيات المنبثقة من نتائجها.

المراجع

أولاً: المراجع العربية

القرآن الكريم.

أبو شامة، عباس (١٩٩٢م). المعايير النموذجية المطلوبة لرجل الأمن، الرياض: المركز العربي للدراسات الأمنية والتدريب.

أبو شامة، عباس (١٤٢٠هـ). التعريف بالظواهر الإجرامية المستحدثة حجمها أبعادها ونشاطها في الدول العربية، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، (١٤- ١٩) مارس.

إنترنت العالم العربي (١٤٢٣هـ). متوفر: http:/www.iamag.com . (٢٢/ ١٠/ ١٤٢٣هـ).

الإيهم (١٤٢٣هـ). التجسس باستخدام الإنترنت، منظمة قراصنة العرب، متوفر: http://www.arabhackers.org/arabic/spy.html . (٢/ ١٢/ ١٤٢٣هـ).

باتوباره، نواف عبد الله (١٤١٩هـ). منافع والتزامات بطاقة الائتمان، المجلة العربية للدراسات الأمنية والتدريب، ع ٢٥، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

بحر، عبد الرحمن (١٩٩٩م). معوقات التحقيق في جرائم الإنترنت: دراسة مسحة على ضباط الشرطة في دولة البحرين، رسالة ماجستير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

البداينة، ذياب (١٩٩٧م). جرائم الحاسب الدولية، ورقة قدمت في ندوة جرائم الحاسب، معهد التدريب: أكاديمية نايف العربية للعلوم الأمنية، الرياض.

البداينة، ذياب (١٩٩٨م). الأمن الوطني في عصر المعلومات، الجزيرة، ٩٤٢١.

البداينة، ذياب (١٩٩٩م). التطبيقات الاجتماعية للإنترنت، ورقة مقدمة في الدورة التدريبية حول شبكة الإنترنت من منظور أمنى، أكاديمية نايف العربية للعلوم الأمنية.

البداينة، ذياب (١٤٢٠هـ). جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، (١٤- ١٩) مارس.

البداينة، ذياب (١٤٢٢هـ). تصميم وتنفيذ البحوث، محاضرات غير منشورة، أكاديمية نايف العربية للعلوم الأمنية.

برهان، محمد (١٩٨٩م). تحليل وتصميم نظم المعلومات الحاسوبية، عمان: مؤسسة الوراق للنشر والتوزيع.

البشري، محمد الآمين (١٤٢١هـ). التحقيق في جرائم الحاسب والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، ع٣٠، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

البشري، محمد الآمين (١٤٢٣هـ). التحقيق في جرائم الحاسب والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، ع ٣٣، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

البكري، سونيا محمد (١٩٨٥م). نظم المعلومات الإدارية، الإسكندرية: المكتب العربي الحديث.

بوابة التكنولوجيا والاتصالات (١٤٢٣هـ). متوفر:
Http://Www.Gn٤me.Com/Etesalat/Article.Jsp?Art_Id=٤٦٩٢ (١٩/ ٧/ ١٤٢٣هـ).

التعزي، عبد الله علي (١٤١٤هـ). أمن شبكات الحاسبات الآلية الشخصية المحلية، القافلة، مجلد٤٢، ع ١٠، شركة أرامكو السعودية، الدمام.

جامعة الملك عبد العزيز (١٤٢٣هـ). أهداف نظام المعلومات، جامعة الملك عبد العزيز، جدة، متوفر: http://www.kaau.edu.sa/odus/nabza.htm (١١، ٩، ١٤٢٣هـ)

الجودي، سامر (١٤٢٣هـ). نظم المعلومات الجغرافية، مجلة التصميم بالحاسوب متوفر:
http://www.cadmagazine.com/pcmagazine/١٠.ht (٢١/ ٧/ ١٤٢٣هـ).

جويلي احمد (٢٠٠٢م). التحول نحو المنظمة الإلكترونية في الوطن العربي، بحث مقدم لمؤتمر الجمعية العربية للإدارة بالقاهرة، القاهرة (١٥- ٢٠) مارس.

الحازمي، خليل (١٤٢٠هـ). أثر استخدام الحاسوب في أداء الأجهزة الأمنية، دراسة مسحية على حرس الحدود بمدينة الرياض، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

الحماحمي (١٤١٩هـ). الحاسب والمجتمع، محاضرات غير منشورة، جامعة الملك سعود.

حسام الدين، (١٤٢٣هـ). برامج الاختراق، المجلة الإلكترونية، متوفر:
http://web.fares.net/w/.ee٧ec٨c (٢/ ٤/ ١٤٢٣هـ)

الحمادي، بسام (١٤٢٣هـ). إثبات ارتكاب جرائم الإنترنت صعب، الرياض، متوفر:
http://www.alriyadh.com.sa (٧/١/١٤٢٣هـ).

الحويطي، موسى (١٤٢٢هـ). نظم المعلومات، جامعة الزقازيق: كلية التجارة.

خشبة، محمد (١٩٩٢م). نظم المعلومات: المفاهيم، التحليل، التنظيم، موسوعة المعلومات والتكلونوجبا، القاهرة: مطابع الوليد.

داود، حسن (٢٠٠٠م) (أ). الحاسب وأمن المعلومات، الرياض: معهد الإدارة.

داود، حسن (٢٠٠٠م) (ب). جرائم نظم المعلومات، الرياض: أكاديمية نايف العربية للعلوم الأمنية.

داود، حسن (١٤٢٠هـ). أمن نظم المعلومات، مجلة الأمن والحياة، ع ٢١١ (١٩)، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

آل دويس، هادي (١٤٢٠هـ). اتجاهات الضباط والأفراد العاملين في الأجهزة الأمنية نحو استخدام الإنترنت: دراسة مسحية على المديرية العامة على الأمن العام، والدفاع المدني في منطقة الرياض، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

الربيعة، فهد (١٤٢٢هـ). نظام المعلومات الصحية والفوائد المتوقعة منه، الرياض، ١١٩٧٢.

رستم، هشام محمد فريد (١٩٩٤م). الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة، أسيوط: مكتبة الآلات الحديثة.

الرشيدي، علي (٢٠٠٠م). معوقات استخدام نظم المعلومات الحاسوبية في عملية اتخاذ القرارات الأمنية: دراسة تطبيقية على القيادات الوسطى بالأمن العام بمدينة الرياض، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

الرقابي (١٤٢٣هـ). الحكومة الإلكترونية ودورها في تقديم الخدمات العامة في المملكة العربية السعودية، رسالة ماجستير غير منشورة، جامعة الملك سعود.

السحيباني، عبد الله (١٤١٧هـ). كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

سليمان، هشام (١٤٢٢هـ). اختراق المواقع والنظم، إسلام أون لاين، متوفر: www.islamonline.net/Arabic/Science/٢٠٠١/٠٤/Article٢٣.shtml//:http (١٤٢٢/٩/٢٠هـ).

سليم، طارق عبد الوهاب (١٩٩٧م). الجرائم المرتكبة بواسطة الإنترنت وسبل مكافحتها، بحث مقدم إلى الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة، مجلس وزراء لداخلية العرب، تونس، (٧-٩) يوليو.

السامرائي، ابتهال (١٤٢١هـ). آخر اختراق تسبب في سرقة ٥٥,٠٠٠ رقم بطاقة ائتمانية، الرياض: http://www.alriyadh-np.com/rnet/٢٠٠١-٠١-٢٠/proxy.html

السيد، إسماعيل (بدون تاريخ). نظم المعلومات لاتخاذ القرارات الإدارية، الإسكندرية: المكتب العربي الحديث.

شرطة دبي (١٩٩٦م). أعمال الحلقة النقاشية حول الإنترنت من منظور أمني، القيادة العامة لشرطة دبي، دبي.

الشدي، طارق عبد الله (١٤٢١هـ). الآلية البناء الأمني لنظم المعلومات، الرياض: دار الوطن للطباعة والنشر.

الشايع، علي سليمان (١٤٢٤هـ). فاعلية نظم المعلومات في التعليم والتدريب: دراسة مسحية على هيئة التدريس في كلية الملك عبد العزيز الحربية، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

شتا، محمد محمد (٢٠٠١م). فكرة الحماية الجنائية لبرامج الحاسب الآلي، الإسكندرية: دار الجامعة الجديدة للنشر.

الشريف هشام (٢٠٠٢م). التحول نحو المنظمة الإلكترونية في الوطن العربي، بحث مقدم لمؤتمر الجمعية العربية للإدارة بالقاهرة، القاهرة (١٥- ٢٠) مارس.

الشهري، عبد الله محمد (١٤٢٢هـ). المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي: دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية.

صلاح (٢٠٠١م). الجاسوس الخفي. متوفر:
http://daleel.ayna.com/technology/forum/٩٧١٠٧٨٧٤١/index_html

الضحيان، سعود، حسن، عزت (١٤٢٣هـ). معالجة البيانات باستخدام برنامج SSPP ١٠، الجزء الثاني، الرياض: مطابع التقنية للأوفست.

طالب، أحسن (١٤٢٠هـ). الجريمة والعقوبة والمؤسسات الإصلاحية، لبنان: بيروت.

الطويل، علي (١٤٢٣هـ). أخطاء FBA ، الرياض، متوفر:
http://writers.alriyadh.com.sa/kpage.asp?art=٣٧٧٥ ٣

عبد الحميد، محمد فاروق (١٤٢٠هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي، الرياض: أكاديمية نايف العربية للعلوم الأمنية.

عبد المطلب، ممدوح عبد الحميد (٢٠٠١م). جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الإنترنت. الشارقة: مكتبة دار الحقوق.

عبيدات، ذوقان، وعدس، عبد الرحمن، وعبد الحق كايد (٢٠٠١م). البحث العلمي مفهومة وأدواته وأساليبه، الطبعة السابعة، عمان: دار الفكر للطباعة والنشر للتوزيع.

العبد المحسن (١٤٢٣هـ). الاختراق، متوفر: Http://Web.Fares.Net/W/.Ee٧e٨a٦

عبد الرحمن، حمدي (١٩٩٢م)، الحماية القانونية للكيانات المنطقية، رسالة دكتوراه غير منشورة، جامعة عين شمس، القاهرة، جمهورية مصر العربية.

عدس، عمر حسن (١٩٩٥م). جرائم الحاسب الآلي: أشكالها وأساليب مواجهتها، بحث مقدم للمؤتمر التاسع عشر لقادة الشرطة والأمن العرب، مجلس وزراء لداخلية العرب، تونس، (١٦-١٨) يوليو.

العساف، صالح (١٤٢١هـ). المدخل إلى البحث في العلوم السلوكية، الطبعة الثانية، الرياض: العبيكان للطباعة والنشر.

عرب، يونس (٢٠٠٢م). موسوعة القانون وتقنية المعلومات، الإمارات: اتحاد المصارف العربية.

العلي، حمد (١٤٢٢هـ). الاختراق، متوفر:
http://daleel.ayna.com/technology/forum/٩٩٤٦٣٣٤٧٠/index_html (١٨/ ٢/ ١٤٢٢هـ)

عودة أحمد، ملكاوي فتحي (١٩٩٢م). أساسيات البحث العلمي في التربية والعلوم الإنسانية، أربد: مكتبة الكتاني.

عودة، عبد القادر (١٤٠١هـ). التشريع الجنائي الإسلامي، (الجزء الأول)، بيروت: مؤسسة الرسالة.

عوض، محمد محي الدين (١٩٩٣م). جرائم نظم المعلومات، بحث مقدم للحلقة العلمية حول جرائم الحاسب الآلي، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

عيد، محمد فتحي (١٤١٩هـ). الأجرام المعاصر، الرياض: أكاديمية نايف العربية للعلوم الأمنية.

الغامدي، يحيى (١٩٩٩م). بناء نظم معلومات الأجهزة الأمنية: دراسة تطبيقية لنظام وثائق الآلي بالإدارة العامة للحماية المدنية في الدفاع المدني، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

غراب، كامل، حجازي، فادية (١٩٩٩م). نظم المعلومات الإدارية، المنتزه: مكتبة ومطبعة الإشعاع الفنية.

الفنتوخ، عبد القادر (١٤٢١هـ). الإنترنت للمستخدم العربي، الطبعة الثانية، الرياض: العبيكان للطباعة والنشر.

الفنتوخ، عبد القادر (١٤٢٣هـ). المسرح الإلكتروني، الرياض، متوفر:
http://writers.alriyadh.com.sa/kpage.asp?art=٣٧٧٥٣

لجنة المعايير (١٩٩٤م). مبادئ وأسس أمن المعلومات وحمايتها، الرياض: جامعة الملك سعود.

المسند، صالح، المهيني، عبد الرحمن (٢٠٠١م). جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات، المجلة العربية الدراسات الأمنية والتدريب، المجلد ١٥، ع ٢٩ (١٥) أكاديمية نايف العربية للعلوم الأمنية، الرياض.

المصري، أحمد (١٩٨٩م). الاتصالات والقرارات وفاعليتها في الإدارة، الكويت: دار القلم.

محمد، ماجد (١٤٢٢هـ). ما هو الاختراق، (١٨/ ٢/ ١٤٢٢هـ)
http://daleel.ayna.com/technology/forum/٩٧١٠٧٨٧٤١/index_html

مجلة الأمن الإلكترونية (٢٠٠١م). أمن الإنترنت، متوفر: http://safola.com/security.chtml (٢٠٠١/١٢/١٠م)

مجلة الأمن الإلكترونية (٢٠٠٢م). أمن الإنترنت، متوفر: http://safola.com/security.chtml (٢٠٠٢/٣/١٦م)

مجلة الأمن الإلكترونية (١٤٢٣هـ). أمن الإنترنت، متوفر: http://safola.com/security.chtml (١٤٢٣/٩/١٩هـ)

المجلة الإلكترونية (١٤٢٣هـ). اختراق المواقع وطرق الوقاية، متوفر:
http://web.fares.net/w/.ee٧ec٨c (٢/ ٧/ ١٤٢٣هـ)

مجلة عالم الكمبيوتر (١٤٢٣هـ). متوفر:
http://computers.arabcomputing.com/pccomponents.html

معيلي علي (٢٠٠٢م). التحول نحو المنظمة الإلكترونية في الوطن العربي، بحث مقدم لمؤتمر الجمعية العربية للإدارة بالقاهرة، القاهرة. (١٥- ٢٠) مارس

مدينة الملك عبد العزيز للعلوم والتقنية (١٤٢٣هـ). أمن المعلومات، متوفر
http://www.isu.net.sa/ar/saudi٪٢٠internet/information-security-ar.htm (٣/ ٧/ ١٤٢٣هـ).

مندورة، محمد محمود (١٤١٠هـ). الجرائم الحاسوبية، دورة فيروس الحاسب الآلي، الرياض: مكتب الأفاق المتحدة.

المنشاوي محمد عبد الله (١٤٢٤هـ). جرائم الإنترنت في المجتمع السعودي: دراسة تطبيقية على جميع مستخدمي الإنترنت في المملكة العربية السعودية، رسالة غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

موسوعة الكمبيوتر والإنترنت (١٤٢٣هـ). النشر الإلكتروني، متوفر:
http://www.c٤arab.com/showac.php?acid=١٦ (٢/ ٦/ ١٤٢٣هـ).

النويصر، محمد (١٩٩٨م). دور نظم المعلومات في مكافحة الإرهاب: دراسة تطبيقية على بعض الأجهزة الأمنية في المملكة، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

النفيعي، مزيد (١٤٢٣هـ). مقاهي الإنترنت والانحراف إلى الجريمة بين مرتاديها: دراسة تطبيقية على مرتادي مقاهي الإنترنت بالمنطقة الشرقية، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

الهاجري، إياس (١٤٢٣هـ). الحرب المعلوماتية، متوفر: http://www.minshawi.com/eyas٢.htm، (١٤٢٢/٧/٢٣هـ).

الهاجري، إياس (١٤٢٢هـ). جرائم الإنترنت، متوفر: http://www.minshawi.com/eyas١.htm، (١٤٢٢/١٠/١٩هـ).

الهادي، محمد (١٩٨٩م). نظم المعلومات المعاصرة، القاهرة: دار الشروق.

وحدة خدمات الإنترنت (١٤٢٣هـ). إحصائيات، مدينة الملك عبد العزيز للعلوم والتقنية: مركز أمن الشبكات، متوفر: http://www.netsec.org.sa/ar/dwabit.htm (٢/ ١٢/١٤٢٣هـ)

يونس، ثائر (١٩٩٤م). شبكات الحاسوب، بيروت: دار الراتب الجامعية.

يونس، عبد الرزاق (١٩٨٩م). التكنولوجيا، عمان: الجامعة الأردنية

ثانياً: المراجع الإنجليزية

Aims (٢٠٠٢) . [Online]. Available: http://www.aims.cjb.net [١٧. ١٠. ٢٠٠٢].

Arabic hackers (٢٠٠٢) . [Online]. Available.www.arabichackers.com

Arabiat (٢٠٠٢) . [Online]. Available: http://www. Arabiat.com

Barman. S. (November, ٢٠٠١).Writing Information Security Policies , New Riders Publishing, . [Online]. Available:: http://safari.informit.com/١٥٧٨٧٠٢٦٤X

BBC. (٢٠٠٢) [Online]. Available: http://news.bbc.co.uk/hi/arabic/news/newsid.st [٢٩. ٠٢. ٢٠٠٢].

Bequai, August (١٩٧٨). Computer Crime., Toronto: Lexington Books.

Castro, H.(٢٠٠٠, June) Developing & Writing Information Security Policies, London: MIS. Training.

CERT, A, (٢٠٠٢) Security Policy, Procedures, and Practices. [Online]. Available: http://www.cert.org/annual_rpts/cert_rpt_٠١.html#other [٩. ١٠. ٢٠٠٢]

CERT,B , (٢٠٠٢). Incidents and Internet Growth. [Online]. Available: http://www.cert.org/annual_rpts/cert_rpt_٠١.html#other [٧. ١٠. ٢٠٠٢]

CERT, C, (٢٠٠٢). CERT* advisories and other security information. Pittsburgh, PA. . [Online]. Available: http://www.cert.org/. [٢٥. ٩. ٢٠٠٢].

Cisco (٢٠٠٢) . [Online]. Available:: http://www.cisco.com/warp/public/٧٠٧/٢٢.html [٢٣. ٩. ٢٠٠٢].

Comguard (٢٠٠٢). [Online]. Available: http://www.comguard.net/arabic/security-overview.html

Florida Association of Computer Crime Investigators (FACCI) (٢٠٠٢). [Online]. Available http://www.facci.org/ [٢٥. ١٠. ٢٠٠٢].

Geocities (٢٠٠٢) . [Online]. Available: http://www.geocities.com/awdaa٢٠٠٠/ershadat/amneh٤٣٣.htm

Gello, Frank (٢٠٠١). Hackers And Internet [online]. Available: http://www.federalcop.Drei.com/conf.html [٤. ١٠. ٢٠٠٢].

Grabosky, p & Smith, G (١٩٩٨). Crime in the Digital Age, Australia: Transaction Publishers And The Federation Press.

IFS, (٢٠٠٢).International Review of criminal policy- united nation manual on the prevention And control of Computer- related Crime. [online]. Available: http://www.ifs.univie.ac.at/~pr٢gg١/rev٤٣٤٤.html [٤. ١٠. ٢٠٠٢].

Infosys-Sy (٢٠٠٢) . [Online]. Available:: Http://Www.Infosys-Sy.Com/Statstic٢.Htm .

Iugaza (٢٠٠٢) . [Online]. Available:Http://Www.Iugaza.Edu /Units/Computercenterdept.Asp [١٤. ١١. ٢٠٠٢].

Itep, A (٢٠٠٢) . [Online]. Available Http://Www.Itep.Co.Ae/Itportal/Arabic/Content/Educationalcenter/Internetconcepts/Wan.Asp [٢٢. ١٠. ٢٠٠٢].

Itep, B (٢٠٠٢) . [Online]. Available Http://Www.Itep.Co.Ae/Itportal/Arabic/Content/Educationalcenter/Internetconcepts/Intranet.Asp [٢٣. ١٠. ٢٠٠٢].

Itep, C (٢٠٠٢) . [Online]. Available Http://Www.Itep.Co.Ae/Itportal/Arabic/Content/Educationalcenter/Internetconcepts/Extranet.Asp [٢٤. ١٠. ٢٠٠٢].

Itep, D (٢٠٠٢) . [Online]. Available http://www.itep.co.ae/itportal/arabic/Content/EducationalCenter/InternetConcepts/intro.asp [٢٤. ١٠. ٢٠٠٢].

Khalal٢٢ (٢٠٠٢) . [Online]. Available: Http://Www.Khalal٢٢.Org/Hakrs.Htm [٢. ٨. ٢٠٠٢].

Nanoart. (٢٠٠٢) [Online]. Available: http://www.nanoart.f٢s.com/hack /. [٢. ٢. ٢٠٠٢].
Nooraelectronics. (٢٠٠٢) [Online]. Available: http://www. Nooraelectronics.com. [٧. ١. ٢٠٠٢].
Nor٢٠٠٠ (٢٠٠٢). [Online]. Available http://www.nor٢٠٠٠.com/netwrk.htm [١٩. ٦. ٢٠٠٢].

Parker, D (١٩٩٨). Fighting Computer Crime, Wiley.

Ressler, R (١٩٩٧). Computer & Internet Crime Training. [Online]. Available: Http://Www.corpus-delicti.com/ training.html [٢٢. ١٢. ٢٠٠٢].

Rapalus, P.(٢٠٠٢, April). CSI/FBI Computer Crime And Security Survey, Compute Security Institute with the participation of the Federal Bureau of Investigation (FBI) Harrison, San Francisco. [Online]. Available: http://www.gocsi.com/press/٢٠٠٢٠٤٠٧.html [٢٩. ٩. ٢٠٠٢]

Spencer, H, (١٩٩٧). Age of uncontrolled information flow, the information society, vol. (١٣), New York: Crane Russak

TIM, W (١٩٩٨). Profits Embolden Hackers. Internet week (march: ٢٣).

Vacca, John. (١٩٩٦). Internet Security Secrets.USA:IDG Book. Worldwide Inc.

القسم الأول / البيانات العامة

الرقم التسلسلي ☐

الأسئلة من ١ إلى ١٠. ✿

١. حدد وظيفتك الشخصية.

☐ إداري ☐ مبرمج ☐ محلل نظم

☐ مدير قاعدة بيانات ☐ مسئول موقع Web Master ☐ مدير نظام System admin

☐ مهندس شبكات ☐ مدقق Auditor ☐ أخصائي أمن معلومات

٢. ما هو نوع المؤسسة التي تعمل بها؟

☐ قطاع حكومي ☐ قطاع مصرفي

☐ شركة متخصصة في مجال تقنية المعلومات ☐ شركة غير متخصصة في مجال تقنية المعلومات

٣. ما هو عدد أجهزة الحاسب الآلي في المؤسسة التي تعمل بها.

☐ أقل من ١٠٠ ☐ من ١٠٠ إلى ١٠٠٠ ☐ أكثر من ١٠٠٠

٤. قدر نسبة المصروفات على تقنية المعلومات إلى أجمالي ميزانية المؤسسة.

☐ أقل من ١٠٪ ☐ من ١٠٪ إلى أقل من ٣٠٪

☐ من ٣٠٪ إلى ٥٠٪ ☐ أكثر من ٥٠٪

٥. هل تتوفر خدمة الإنترنت لموظفي المؤسسة؟

☐ نعم تتوفر للجميع ☐ تتوفر لبعض الموظفين فقط ☐ لا تتوفر

٦. ما هو أسلوب الدخول لشبكة الإنترنت في المؤسسة التي تعمل بها؟

☐ الخطوط الهاتفية (dial up) ☐ الشبكة المحلية المربوطة بمزود الخدمة

☐ شبكة خاصة مستقلة عن شبكة العمل ☐ لا يوجد إطلاقاً

٧. هل يوجد في المؤسسة التي تعمل بها سياسة أمنية للتعامل مع الحاسبات الآلية والإنترنت؟

☐ نعم ☐ لا ☐ لا أدري

٨. هل يوجد في المؤسسة التي تعمل بها قسم متخصص في أمن المعلومات؟

☐ نعم ☐ لا ☐ لا أدري

٩. إذا كان يوجد قسم خاص في أمن المعلومات بالمؤسسة التي تعمل بها فكم عدد العاملين في القسم.

☐ ١ ☐ من ٢ إلى ٥ ☐ من ٦ إلى ١٠

☐ من ١١ إلى ٢٠ ☐ من ٢١ إلى ٥٠ ☐ أكثر من ٥٠

القسم الثاني/ البيانات التفصيلية

١. قيم كل عبارة من العبارات التالية المتعلقة بالسياسة الأمنية بمؤسستكم.					◌ ✿ ◉
العنصر	مدى الموافقة				
	أوافق بشدة	أوافق	موافق إلى حد ما	لا أوافق	لا أوافق إطلاقا
١٠. توجد سياسة أمنية Policy Security واضحة لأمن نظم المعلومات بالمؤسسات					
١١. توجد سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية					
١٢. يتقيد الرؤساء بالسياسة الأمنية عند إعطاء التعليمات					
١٣. يلزم الموظفين بالسياسة الأمنية يوضع عقوبات للمخالفين					
١٤. يتم إعلان السياسة الأمنية للموظفين بما يكفل تبليغها للعموم					

٢. حدد مدى وجود العناصر التالية في السياسة الأمنية للمؤسسات.					◌ ✿ ◉
العنصر	التقييم				
	موجود وواضح	موجود وغير واضح	ليس موجود وضرورياً	ليس موجود وغير ضرورياً	لا أدري
١٥. الجانب البشري					
١٦. الموقع المكاني لخدمات تقنية المعلوماتية					
١٧. البرامج المطورة داخلياً					
١٨. البرامج الجاهزة					
١٩. استخدام الإنترنت					
٢٠. التشارك في الخدمات					
٢١. االإحترازات الشخصية					
٢٢. الوثائق ووسائط الحفظ					

٢٣. ما أهمية وجود إجراءات إدارية و فنية لأمن نظم المعلومات؟	✿
☐ مهم جداً	☐ مهم
☐ مهم إلى حداً ما	☐ غير مهم
☐ غير مهم على الإطلاق	

٢٤. كيف تتم التوعية في مجال أمن المعلومات للعاملين في المؤسسة التي تعمل بها؟	✿
☐ نشرات داخلية	☐ مجلات ودوريات ومراجع
☐ ندوات ومحاضرات	☐ لا توجد

۳. فضلاً حدد مدى أتباع إجراءات أمن المعلومات في المؤسسات.					✪
العنصر	التقييم				
	دائماً	غالباً	أحياناً	نادراً	لا يتبع إطلاقاً
٢٥. التدريب الدوري على أمن المعلومات					
٢٦. الالزام العاملين بالنظم الإدارية المحددة					
٢٧. منح الحوافز للالتزام بالإجراءات الأمنية					
٢٨. توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم					
٢٩. الطلاب ممن يلتحق حديثاً بالخدمة تزكية كشرط للتوظيف					
٣٠. عدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين					
٣١. استخدام التقنية للدخول على الأنظمة (بصمة الإصبع، بصمة العين)					
٣٢. توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها					
٣٣. الإجراءات الأمنية لصيانة الأجهزة					
٣٤. الإجراءات التي تكفل أمن النسخ الاحتياطي ووسائط الحفظ الخارجية					
٣٥. إجراءات تحديث النسخ الاحتياطي المركزي					
٣٦. تحديد مدة صلاحية كلمات المرور وتغييرها					
٣٧. التأكد من مزامنة ساعات الأجهزة باستمرار					
٣٨. اختيار نوعية مناسبة من وسائل الحماية تلائم نوع التطبيق					
٣٩. تحديث برامج الحماية باستمرار					
٤٠. التقدم بشكوى حول جرائم نظم المعلومات					
٤١. تشكيل فريق طوارئ للتعامل مع الجريمة					
٤٢. رصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم					
٤٣. استخدام وسائل حماية تساعد في تتبع المجرمين					
٤٤. ربط الترقية والدورات (الحوافز الأخرى) بمدى التقيد بأمن المعلومات					
٤٥. الضوابط الأمنية لبناء وتشغيل البرامج التطبيقية					
٤٦. الضوابط المنظمة لعمليات التشغيل					
٤٧. ضوابط مبرمجي قواعد البيانات ومدرائها					
٤٨. ضوابط إدارة الشبكات وخطوط الاتصال					
٤٩. ضوابط عمليات الإدخال والإخراج					

٥٠. تحدث جرائم نظم المعلومات في مؤسستكم بشكل.		✪
☐ يومي على الأقل	☐ أسبوعي على الأقل	☐ شهري على الأقل
☐ سنوي على الأقل	☐ غير منتظم	☐ لا أدري

٥١. في حالة حدوث جرائم نظم المعلومات عن طريق الإنترنت في مؤسستكم بشكل أسبوعي فإن عدد الإنذارات في بعض الأحيان تصل إلى:		✪
☐ أقل من ١٠	☐ من ١٠ إلى أقل من ١٠٠	☐ من ١٠٠ إلى أقل من ١٠٠٠

	☐ من ١٠٠٠ إلى أقل من ١٠٠٠٠	☐ من ١٠٠٠٠ إلى ٥٠٠٠٠	☐ أكثر من ٥٠٠٠٠

٤. الرجاء تقييم مدى حدوث كل جريمة من الجرائم التالية في المؤسسات.

العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا يوجد
٥٢. التلاعب بإدخال البيانات					
٥٣. تغيير البرامج والإعدادات					
٥٤. تغيير البيانات بعد إدخالها					
٥٥. تدمير الملفات وقواعد البيانات					
٥٦. تعطيل المواقع والبرامج والأجهزة					
٥٧. التنصت وسرقة البيانات					
٥٨. نسخ البيانات للاستفادة منها					
٥٩. نسخ البرامج والاستخدام غير المصرح به					
٦٠. الاستيلاء على ما سوى المعلومات بالمؤسسة، كالأرقام السرية والبرامج					
٦١. إرسال أحصنة طروادة					
٦٢. إرسال وزراعة فيروسات					
٦٣. الاختراقات للبريد الإلكتروني					
٦٤. اعتراض الرسائل والتنصت على الشبكات					
٦٥. إغراق البريد الإلكتروني					

٥. الرجاء اختيار التقييم المناسب لكل فقرة.

العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا يوجد
٦٦. مدى خطورة جرائم نظم المعلومات					
٦٧. معدل جرائم نظم المعلومات بعد ظهور الإنترنت					
٦٨. حجم الجرائم التي تم الإعلان عنها في مؤسستكم					
٦٩. حجم جرائم نظم المعلومات مقارنة بحجم الجرائم الأخرى في المؤسسة التي تعمل بها					

٦. الرجاء اختيار التقييم المناسب لكل فقرة.

العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا يوجد
٧٠. قدر الجهد المبذول لمتابعة جرائم نظم المعلومات من قبل قسم خاص بالمؤسسة					
٧١. الاعتماد على ضمانات موردي الأجهزة والبرامج بدلاً من تتبع الجرائم					
٧٢. حجم اهتمام الجهة الأمنية بعد الإبلاغ عن الجريمة المعلوماتية					
٧٣. جرائم نظم المعلومات التي اكتشفت دون ضبط ملابساتها					

٧٤. جرائم نظم المعلومات التي اكتشفت وضبطت ملابساتها					
٧٥. الجرائم التي تم ضبطها ومعرفة مصدرها وآثارها في مؤسستكم					

٧. قدر مدى استخدام كل أسلوب من الأساليب التالية في ارتكاب جرائم نظم المعلومات التي تتعرض لها المؤسسات.

العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا يوجد
٧٦. استخدام برامج حديثة تقوم باستغلال نقاط الضعف في برامج الحماية					
٧٧. إرسال الفيروسات المدمرة بالبريد الإلكتروني أو برامج المحادثة وما شابهها					
٧٨. إرفاق أحصنة طروادة بالبرامج					
٧٩. IP Spoofing					
٨٠. انتحال شخصية عبر البريد الإلكتروني					
٨١. محاولة اكتشاف المنافذ المفتوحة والدخول منها إلى الجهاز					
٨٢. النفاذ عبر الشبكة إلى الأجهزة ومحاولة العثور على ملفات مشاركة غير محمية					
٨٣. استغلال الثغرات التي تكتشف في نظم التشغيل والتطبيقات العاملة معه					
٨٤. استغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة					
٨٥. برمجة النظم والتطبيقات بطريقة تحقق للمبرمج مصالح شخصية غير مشروعة					
٨٦. إرفاق الملفات (ذاتية التشغيل/ بحاجة إلى تشغيل) والتي تقوم بعمليات تخريبية					
٨٧. التخفي تحت البرامج المجانية والمواقع الجذابة للحصول على معلومات عن الزائر					
٨٨. استغلال الثغرات الأمنية في مزودات الويب Web Servers مثل مزود IIS					
٨٩. سرقة وسائط الحفظ الخارجية نتيجة تساهل العاملين بالمؤسسة					
٩٠. تشغيل الجهاز عن طريق القرص المرن للدخول الغير مرخص على الأقراص					
٩١. ترك أقراص مرنة ملوثة بالفيروسات					
٩٢. زراعة برامج اختراق بواسطة موظفي الصيانة والتشغيل بالمؤسسة					
٩٣. الحصول على البيانات السرية خلال أعمال صيانة الأجهزة					
٩٤. الاستخدام غير قانوني لأجهزة الغير حين تركها غير مؤمنة					

٩٥. قدّر التكلفة المالية لجرائم نظم المعلومات المترتبة عليها بالنسبة إلى أجمالي مصروفات المؤسسة.

☐ أقل من ٥٪	☐ من ٥٪ إلى أقل من ١٠٪	☐ من ١٠٪ إلى أقل من ٣٠٪
☐ من ٣٠٪ إلى ٥٠٪	☐ أكثر من ٥٠ ٪	

٨. حدد حجم استخدام كل من المنافذ التالية لارتكاب الجرائم ضد المؤسسة.

العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا يوجد
٩٦. إفشاء الرقم السري من قبل الموظفين					
٩٧. المحاولة المتكررة					
٩٨. استخدام برامج فك التشفير					
٩٩. عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد					

١٠٠.عن طريق الأجهزة ومحركات الأقراص المرنة والليزر					
١٠١.عن طريق الشبكة الواسعة WAN والبرامج المرتبطة بها					
١٠٢.عن طريق شبكة الإنترنت وبرامج الاختراق الموجودة بها					
١٠٣.عن طريق شبكة VPN والبرامج التي تعمل عليها					

٩. إلى أي مدى تستخدم كل أداة من الأدوات التالية في ارتكاب جرائم نظم المعلومات في المؤسسات؟					
العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا يستخدم
١٠٤. cookies					
١٠٥. Marker Groove					
١٠٦. Caligula					
١٠٧. Net Bus					
١٠٨. Sub Seven					
١٠٩. Hack a Tack					
١١٠. Win Crash					
١١١. برنامج icq					
١١٢. Tribe Flood Network (TFN)					
١١٣. Password Recovery Toolkit					
١١٤. MS Word Cracker					
١١٥. MS Excel Cracker					
١١٦. Revelation					
١١٧. برامج التنصت على الشبكات					
١١٨. أقراص بدء التشغيل					
١١٩. المشاركة في الملفات على الشبكة					
١٢٠. البريد الإلكتروني					
١٢١. الفيروسات وديدان الإنترنت					

١٠. كيف تقدر حجم الحصول على الأدوات المستخدمة في ارتكاب جرائم نظم من قبل مجرمي نظم المعلومات بالمملكة.					
العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا أدري
١٢٢. محلات بيع البرامج المرخصة					
١٢٣. أماكن بيع البرامج الغير قانونية					
١٢٤. البرامج المجانية التي يتم الحصول عليها من مواقع على الإنترنت					
١٢٥. البرامج الغير مجانية التي تشترى من مواقع على شبكة الإنترنت					

١١. قيم كل دافع من دوافع جرائم نظم المعلومات لارتكاب الجرائم بالمؤسسات.					
العنصر	التقييم				
	عالي جداً	عالي	متوسط	محدود	لا يوجد
١٢٦. سياسية وعسكرية					
١٢٧. إبراز القدرات					

١٢٨. التسلية وحب الاستطلاع					
١٢٩. اقتصادية وتجارية					
١٣٠. الانتقام					
١٣١. الوصول إلى معلومات شخصية					

١٢. حدد مدى صحة كل عبارة من العبارات التالية.

العنصر	التقييم			
	دائماً	غالباً	أحياناً	نادراً
١٣٢. من الممكن استخدام تقنية المعلومات كوسيلة من وسائل ضبط الجريمة والتحقيق فيها				
١٣٣. اعتبار برامج الحماية وسيلة ضبط وتحقيق هامة				
١٣٤. تستطيع المؤسسة المستهدفة من قبل مجرمي نظم المعلومات تحديد مصدر الهجوم (داخلي، خارجي)				
١٣٥. المؤسسة المستهدفة من قبل مجرمي نظم المعلومات لا تستطيع تحديد مصدر الأدوات المستخدمة في الجريمة				

١٣٦. يمكن التعرف على شخصية مرتكب جريمة نظم المعلومات بالمؤسسة باستخدام:		۞ ۞
	☐ وسائل أمن البيانات	☐ تعقب إجراءات أمن العاملين

١٣٧.يمكن التعرف على شخصية مرتكب جريمة نظم المعلومات بالمؤسسة بواسطة:	۞ ۞
☐ عنوانIP	☐ استخدام وسائل تتبع المخترقين
☐ برامج الحماية	☐ برامج تتبع مصدر الرسائل الإلكترونية

١٣٨. تساعد برامج الحماية في:	۞ ۞
☐ تحديد نوع الجريمة المرتكبة	☐ تحديد توقيت ارتكاب الجريمة
☐ الإعلام بوجود جريمة مرتكبة	☐ تحديد مصدر الجريمة

١٣. في حالة الإحجام عن الإبلاغ عن الجرائم المعلوماتية حدد مدى تأثير كل سبب من الأسباب التالية: ۞ ۞

العنصر	التقييم				
١٣٩. الحفاظ على السمعة	ي جداً	عالي	وسط	محدود	لا يوجد
١٤٠. عدم إبراز كفاءة المجرمين					

١٤١. الخوف من المسؤولية					
١٤٢. عدم الرغبة في الظهور بمظهر الضحية					
١٤٣. عدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع					
١٤٤. محدودية الآثار المترتبة على الجريمة					

١٤. حدد مدى أهمية كل من أدوات المساعدة بضبط الجريمة					◌ ✿ ◉
العنصر	التقييم				
	مهم جداً	مهم	مهم إلى حداً ما	غير مهم	غير مهم إطلاقاً
١٤٥. سجل الصلاحيات للمستخدمين					
١٤٦. أدوات المراجعة Auditing					
١٤٧. أدوات مراقبة المستخدمين للشبكة					
١٤٨. أدوات التنصت على الشبكة					
١٤٩. لتقارير (Reporting) التي تنتجها نظم أمن البيانات					
١٥٠. مراجعة قاعدة البيانات					
١٥١. تقارير الجدران النارية Reporting					
١٥٢. برامج تتبع المخترقين					
١٥٣. برامج تتبع مصدر إرسال الرسائل الإلكترونية					
١٥٤. برامج كسر كلمة المرور					
١٥٥. برامج كشف الفيروسات					
١٥٦. برامج النسخ الاحتياطي والتسجيل Logging					

١٥. حدد مدى أهمية كل من أدوات المساعدة بالتحقيق فيها					◌ ✿ ◉
العنصر	التقييم				
	مهم جداً	مهم	مهم إلى حداً ما	غير مهم	غير مهم إطلاقاً
١٥٧. أداة فك التشفير					
١٥٨. أدوات استرجاع المعلومات من الأقراص التالفة مثل View disk					
١٥٩. برامج الضغط وفك الضغط Pkzip					
١٦٠. برامج كسر كلمة المرور					
١٦١. برامج البحث عن الملفات العادية والمخفية مثل Xtreepro gold					
١٦٢.برامج اتصالات مثل Lantastic					

١٦٣. برامج تشغيل الحاسب مثل Bootable diskette					
١٦٤. برامج نسخ البيانات مثل Lap link					
١٦٥. برامج مقارنة النسخ					
١٦٦. برامج النسخ الاحتياطي والتسجيل Logging					

١٦. إذا كنت ترى أن كل عبارة من العبارات التالية تمثل عائقاً للتحقيق فحدد مدى توفر الكفاءة البشرية القادرة على تحقيق العناصر التالية في المؤسسة التي تعمل بها.					◌
العنصر	التقييم				
	عالية جداً	عالية	متوسطة	محدودة جداً	لا توجد
١٦٧. المهارة العالية لاستخدام الحاسب الآلي والإنترنت					
١٦٨. المعرفة بمتطلبات أمن المعلومات					
١٦٩. المقدرة على إتباع السياسة الأمنية للتعامل مع الجرائم					
١٧٠. المعرفة بأساليب ارتكاب جرائم نظم المعلومات					
١٧١. المقدرة على الإثبات الجنائي لجرائم نظم المعلومات					
١٧٢. المهارة العالية لاستخدام الحاسب الآلي والإنترنت					

١٧. إذا كنت ترى أن كل عبارة من العبارات التالية تمثل عائقاً للتحقيق فحدد مدى توفر المتطلبات الآتية.				◌✪
العنصر	التقييم			
	متوفر ومستخدم	متوفر غير مستخدم	غير متوفر ولكن ضرورياً	ليس ضرورياً
١٧٣. التنسيق بين المؤسسات المستخدمة للنظم والموفرة للأمن				
١٧٤. التنسيق بين والجهات الأمنية والمؤسسات المستخدمة للنظم				

١٨. إذا كنت ترى أن كل عبارة من العبارات التالية تمثل عائقاً للتحقيق فحدد مدى توفرها.				◌
العنصر	التقييم			
	متوفر ومستخدم	متوفر غير مستخدم	غير متوفر ولكن ضرورياً	ليس ضرورياً
١٧٥. توفير الأجهزة والبرامج المناسبة للتحقيق				

١٧٦. المتخصصين والخبراء في الحاسب الآلي				
١٧٧. التدريب في معاهد متخصصة بالتحقيق في جرائم النظم				

١٩. حدد مدى صحة كل عبارة من العبارات التالية					۞ ◌
العنصر	مدى الموافقة				
	موافق بشدة	موافق	موافق إلى حد ما	غير موافق	غير موافق بشدة
١٧٨. لا يوجد تشريعات واضحة خاصة بجرائم نظم المعلومات في البلاد					
١٧٩. مكونات عناصر جريمة نظم المعلومات غير معروفة للأطراف المعنية بالجريمة					
١٨٠. لا يوجد متخصص في جرائم المعلوماتية لديكم					
١٨١. لا توجد متابعة المستجدات حول جرائم نظم المعلومات					
١٨٢. عدم وجود مردود مادي ملحوظ لتحديث برامج الحماية والتحقيق					
١٨٣. لا توجد قناعة لدى العاملين في مجال نظم المعلومات بتدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية					
١٨٤.معظم المؤسسات المتضررة من جرائم نظم المعلومات لا تتقدم بشكوى للجهات الرسمية					
١٨٥. يقاوم الموظفين الوسائل الأمنية للإبقاء على قدر من الحرية					
١٨٦. عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق					
١٨٧.عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين					
١٨٨. لا تتم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات					
١٨٩. تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية					
١٩٠. إمكانية ارتكاب هذه الجرائم عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط					

٢٠. ما مدى أهمية الدليل الإلكتروني في إثبات ارتكاب جريمة ما من قبل مجرمي نظم المعلومات؟	◌
العنصر	التقييم

	مهم جداً	مهم	مهم إلى حداً ما	غير مهم	غير مهم إطلاقاً
١٩١. تسجيل الوقائع Logging					
١٩٢. التغير الظاهر على البرامج.					
١٩٣. وجود فيروسات.					
١٩٤. وجود أحصنة طروادة Trojan Horses					

	العينة	الوظيفة	المؤسسة	v3	الأنترنت	الاسلوب	مصروفات
1	1.00	8.00	3.00	3.00	2.00	2	3
2	1.00	5.00	3.00	3.00	1.00	2	4
3	1.00	6.00	3.00	3.00	1.00	2	4
4	1.00	1.00	3.00	3.00	1.00	2	4
5	1.00	2.00	3.00	3.00	1.00	2	4
6	1.00	8.00	3.00	3.00	2.00	2	4
7	1.00	8.00	3.00	3.00	2.00	2	4
8	1.00	8.00	3.00	3.00	1.00	2	3
9	1.00	6.00	3.00	3.00	1.00	2	2
10	1.00	8.00	3.00	3.00	1.00	2	4
11	1.00	6.00	3.00	3.00	2.00	2	4
12	1.00	7.00	3.00	3.00	1.00	2	3
13	1.00	5.00	3.00	3.00	1.00	2	3
14	1.00	4.00	3.00	3.00	2.00	2	3
15	1.00	8.00	3.00	3.00	2.00	2	3
16	1.00	3.00	3.00	3.00	2.00	2	3
17	1.00	5.00	3.00	3.00	2.00	2	4
18	1.00	4.00	3.00	2.00	2.00	2	2
19	1.00	8.00	3.00	2.00	2.00	2	3
20	1.00	9.00	3.00	3.00	1.00	2	4
21	1.00	2.00	3.00	1.00	2.00	2	1
22	1.00	2.00	3.00	1.00	2.00	2	1
23	1.00	8.00	3.00	3.00	2.00	2	4
24	1.00	8.00	3.00	2.00	2.00	2	4
25	1.00	2.00	3.00	3.00	1.00	2	4
26	1.00	8.00	3.00	1.00	2.00	2	3
27	1.00	5.00	3.00	1.00	1.00	2	3
28	1.00	1.00	3.00	1.00	2.00	2	3
29	1.00	1.00	3.00	1.00	2.00	2	1
30	1.00	1.00	3.00	1.00	2.00	2	2
31	1.00	7.00	3.00	1.00	1.00	2	2
32	1.00	1.00	3.00	1.00	1.00	2	2
33	1.00	2.00	3.00	1.00	1.00	2	1
34	1.00	2.00	3.00	1.00	1.00	2	2
35	1.00	8.00	1.00	3.00	2.00	2	2
36	1.00	3.00	1.00	2.00	1.00	2	3
37	1.00	9.00	1.00	2.00	2.00	2	3
38	1.00	6.00	1.00	2.00	1.00	2	3
39	1.00	6.00	1.00	2.00	1.00	2	3
40	1.00	3.00	1.00	2.00	1.00	2	3
41	1.00	3.00	1.00	2.00	1.00	2	3
42	1.00	8.00	1.00	2.00	2.00	2	3
43	1.00	1.00	1.00	2.00	1.00	2	3
44	1.00	1.00	1.00	2.00	1.00	2	3
45	1.00	3.00	1.00	2.00	1.00	2	3
46	1.00	1.00	4.00	1.00	2.00	1	1
47	1.00	9.00	4.00	1.00	2.00	3	3
48	1.00	3.00	4.00	1.00	2.00	1	3
49	1.00	1.00	4.00	1.00	2.00	2	1
50	1.00	1.00	4.00	1.00	2.00	1	1

	قسم	العاملين	سياسة	حدوث	v11	v12	v13
1	1	5	1.00	5.00	5	4	5
2	1	4	1.00	1.00	5	3	4
3	1	4	1.00	1.00	5	4	4
4	1	3	1.00	1.00	5	4	4
5	1	5	1.00	4.00	5	2	2
6	1	5	1.00	5.00	5	4	5
7	1	5	1.00	5.00	5	4	5
8	1	3	1.00	5.00	5	4	5
9	1	4	1.00	1.00	5	5	4
10	1	5	1.00	5.00	5	4	5
11	1	5	1.00	5.00	5	5	5
12	1	3	1.00	1.00	5	4	4
13	1	4	1.00	1.00	5	4	4
14	1	4	1.00	5.00	5	3	5
15	1	5	1.00	5.00	5	4	5
16	1	5	1.00	1.00	5	4	4
17	1	5	1.00	5.00	5	4	5
18	2	.	1.00	6.00	5	4	4
19	2	.	1.00	6.00	5	4	5
20	1	5	1.00	1.00	5	3	4
21	2	.	2.00	6.00	5	4	4
22	2	.	2.00	6.00	5	2	5
23	1	4	1.00	5.00	5	4	5
24	1	4	1.00	5.00	5	2	5
25	1	4	1.00	1.00	5	4	4
26	1	4	1.00	5.00	5	4	5
27	1	4	1.00	1.00	5	2	4
28	2	.	2.00	5.00	5	4	5
29	2	.	2.00	1.00	5	2	4
30	2	.	2.00	1.00	5	2	4
31	2	.	2.00	1.00	5	2	4
32	2	.	1.00	1.00	5	2	4
33	2	.	1.00	1.00	5	2	4
34	1	2	1.00	4.00	5	4	2
35	1	2	1.00	5.00	5	4	5
36	1	3	1.00	4.00	5	3	5
37	1	3	1.00	5.00	5	5	4
38	1	3	1.00	4.00	5	3	4
39	1	3	1.00	4.00	5	3	4
40	1	3	1.00	4.00	5	3	4
41	1	2	1.00	4.00	5	3	4
42	1	2	1.00	5.00	5	5	1
43	1	3	1.00	4.00	5	3	2
44	1	4	1.00	4.00	5	3	2
45	1	4	1.00	4.00	5	3	4
46	1	1	2.00	5.00	5	3	3
47	1	2	1.00	5.00	5	4	4
48	2	.	2.00	5.00	5	4	5
49	2	.	1.00	5.00	5	4	4
50	2	.	2.00	5.00	4	3	5

	v14	v15	v16	v17	v18	v19	v20
1	5	5	3	4	1	3	3
2	4	5	3	3	3	4	4
3	4	5	3	3	3	4	2
4	4	5	3	3	3	4	1
5	5	5	2	2	5	2	4
6	5	5	3	4	4	3	3
7	5	5	3	4	4	3	3
8	5	5	3	4	4	3	3
9	4	4	3	3	3	4	4
10	5	5	3	1	4	3	3
11	5	5	3	1	1	3	3
12	4	5	3	3	3	4	4
13	4	5	3	3	3	4	4
14	5	5	3	4	4	3	3
15	5	5	3	1	4	3	3
16	4	5	3	3	3	4	4
17	5	5	3	4	4	3	3
18	4	5	3	3	3	4	4
19	5	5	3	4	4	3	3
20	4	5	3	3	3	3	4
21	5	5	2	4	5	3	4
22	5	5	2	2	5	4	4
23	5	5	3	4	4	3	3
24	5	5	3	4	4	3	3
25	4	5	3	3	3	2	4
26	5	5	3	4	4	3	3
27	4	5	3	3	3	2	4
28	5	5	3	4	4	3	3
29	5	5	3	3	3	2	4
30	5	5	3	3	3	4	4
31	4	5	3	3	1	2	4
32	4	5	3	3	3	4	4
33	5	5	3	3	3	2	4
34	5	5	2	2	1	4	4
35	5	5	3	4	1	3	3
36	4	4	4	2	1	1	2
37	4	5	2	1	1	1	1
38	5	5	4	2	1	1	2
39	5	5	4	2	1	1	2
40	5	5	4	2	1	2	2
41	5	5	4	2	1	1	2
42	5	5	2	1	1	3	1
43	5	5	4	2	5	1	2
44	4	3	4	2	4	1	2
45	5	3	4	2	5	1	2
46	4	5	3	4	4	3	4
47	5	5	3	4	1	3	4
48	5	5	3	4	4	2	3
49	5	4	3	2	4	2	4
50	5	5	3	4	4	2	4

	v21	التلاعب	البرامج	البيانات	تدمير	تعطيل	تنصت
1	2	5	4	4.00	3	3	3
2	3	5	4	5.00	4	3	3
3	3	5	4	5.00	4	3	3
4	3	5	4	5.00	4	3	3
5	4	1	5	1.00	4	1	2
6	4	4	4	4.00	3	3	3
7	4	5	4	4.00	3	3	3
8	4	5	4	4.00	3	3	3
9	3	4	4	5.00	2	3	3
10	4	5	4	4.00	3	3	2
11	4	4	4	4.00	3	3	3
12	3	5	5	5.00	4	3	3
13	3	5	4	5.00	2	4	3
14	4	2	4	4.00	3	3	3
15	4	4	5	4.00	3	3	3
16	3	5	5	5.00	3	3	4
17	4	5	5	4.00	5	1	3
18	3	5	5	5.00	4	3	4
19	4	5	5	4.00	3	3	3
20	3	5	5	5.00	2	3	3
21	4	1	5	1.00	4	1	4
22	4	1	5	1.00	4	1	2
23	4	5	4	4.00	3	3	3
24	4	5	4	4.00	3	3	4
25	3	5	4	5.00	4	3	3
26	4	5	5	4.00	3	1	3
27	3	5	4	5.00	4	3	3
28	4	3	4	4.00	3	3	3
29	3	3	4	5.00	2	4	4
30	3	4	5	5.00	4	3	3
31	3	4	5	5.00	3	1	3
32	3	5	5	5.00	2	3	4
33	3	4	5	5.00	3	3	3
34	4	1	5	1.00	4	1	4
35	4	5	4	4.00	3	3	3
36	3	4	2	1.00	4	1	3
37	1	4	4	1.00	1	1	1
38	3	2	2	1.00	4	4	3
39	3	4	2	1.00	4	4	1
40	3	4	2	3.00	4	4	3
41	3	4	2	1.00	4	1	1
42	1	4	4	1.00	4	2	1
43	3	2	2	2.00	5	1	1
44	3	4	4	1.00	5	4	1
45	3	4	2	1.00	5	4	1
46	4	5	4	4.00	3	1	3
47	4	5	4	4.00	3	3	3
48	4	5	4	4.00	4	1	3
49	4	4	5	4.00	3	2	3
50	4	5	4	4.00	4	3	3

	نسخ	برامجها	استيلاء	أحصنة	فيروسات	أختراقات	إعتراض
1	4	5	4	4	5	3	3
2	3	3	4	4	5	4	4
3	3	3	4	4	5	4	4
4	3	3	4	4	5	4	4
5	1	2	1	5	1	1	3
6	4	5	4	4	5	3	3
7	4	5	4	4	5	3	3
8	4	5	4	4	5	3	3
9	3	3	2	4	5	4	2
10	4	5	2	5	5	3	3
11	4	5	4	4	5	3	3
12	3	3	4	4	5	4	4
13	3	3	4	4	5	4	4
14	4	5	4	4	5	3	3
15	2	5	4	4	5	3	3
16	3	3	4	4	5	4	4
17	4	5	4	4	5	3	3
18	3	3	4	4	5	4	4
19	4	5	4	2	5	3	3
20	3	3	4	4	5	4	4
21	3	2	1	4	1	1	3
22	1	2	1	4	1	1	3
23	4	5	4	4	5	3	3
24	4	5	4	4	5	3	3
25	3	3	4	4	5	4	4
26	4	5	4	4	5	3	3
27	3	3	4	4	5	4	4
28	4	5	4	4	5	3	3
29	3	3	4	4	5	4	4
30	3	3	4	4	5	4	4
31	3	3	4	4	5	4	4
32	3	3	4	4	5	4	4
33	3	3	4	4	5	4	4
34	1	2	3	4	1	1	3
35	4	5	3	4	5	3	3
36	1	2	1	1	1	2	3
37	3	2	3	2	2	1	1
38	1	2	3	4	1	2	3
39	4	2	3	4	1	1	3
40	3	2	3	2	5	2	3
41	1	2	4	4	3	1	3
42	2	2	4	2	2	2	3
43	1	4	3	2	3	1	3
44	1	2	5	2	3	1	3
45	1	2	4	4	3	2	3
46	4	5	4	4	5	3	3
47	4	5	4	4	5	3	3
48	4	4	4	4	5	3	3
49	4	5	4	4	5	3	3
50	4	5	4	4	5	3	3

	إغراق	أفشاء	محاولة	فك	lan	الأقرص	wan
1	3	5.00	5.00	4.00	4.00	4.00	4.00
2	3	5.00	4.00	4.00	3.00	3.00	3.00
3	3	5.00	4.00	3.00	3.00	3.00	3.00
4	3	5.00	4.00	3.00	3.00	3.00	3.00
5	1	3.00	3.00	1.00	5.00	4.00	2.00
6	3	5.00	5.00	4.00	4.00	4.00	4.00
7	2	5.00	5.00	4.00	4.00	4.00	4.00
8	2	5.00	5.00	4.00	4.00	4.00	4.00
9	3	5.00	4.00	3.00	5.00	3.00	3.00
10	3	5.00	5.00	4.00	4.00	4.00	4.00
11	3	5.00	5.00	4.00	4.00	4.00	4.00
12	2	5.00	4.00	3.00	5.00	3.00	3.00
13	3	5.00	4.00	3.00	5.00	3.00	3.00
14	3	5.00	5.00	4.00	4.00	4.00	4.00
15	3	5.00	5.00	4.00	4.00	5.00	4.00
16	3	5.00	4.00	3.00	5.00	5.00	3.00
17	3	5.00	5.00	4.00	4.00	5.00	4.00
18	3	5.00	4.00	3.00	3.00	5.00	3.00
19	3	5.00	5.00	4.00	4.00	5.00	4.00
20	3	5.00	4.00	3.00	3.00	5.00	3.00
21	1	3.00	5.00	1.00	5.00	5.00	2.00
22	1	3.00	5.00	1.00	5.00	4.00	2.00
23	2	5.00	5.00	2.00	4.00	5.00	4.00
24	3	5.00	5.00	4.00	4.00	5.00	4.00
25	3	5.00	4.00	3.00	4.00	5.00	3.00
26	2	5.00	5.00	4.00	4.00	5.00	4.00
27	3	5.00	4.00	3.00	3.00	5.00	3.00
28	3	5.00	5.00	4.00	4.00	4.00	4.00
29	3	5.00	4.00	3.00	5.00	3.00	3.00
30	3	5.00	4.00	3.00	3.00	3.00	3.00
31	3	5.00	4.00	3.00	3.00	3.00	3.00
32	3	5.00	4.00	3.00	3.00	3.00	3.00
33	3	5.00	4.00	3.00	3.00	3.00	3.00
34	1	3.00	4.00	1.00	5.00	5.00	2.00
35	3	5.00	5.00	4.00	4.00	4.00	4.00
36	1	3.00	4.00	1.00	5.00	5.00	2.00
37	1	1.00	2.00	1.00	4.00	5.00	1.00
38	1	3.00	4.00	1.00	5.00	5.00	2.00
39	2	3.00	4.00	1.00	4.00	5.00	2.00
40	1	3.00	1.00	1.00	4.00	5.00	2.00
41	1	3.00	1.00	1.00	4.00	1.00	2.00
42	1	1.00	2.00	1.00	4.00	5.00	1.00
43	1	3.00	1.00	1.00	5.00	5.00	2.00
44	1	3.00	1.00	1.00	4.00	4.00	2.00
45	3	3.00	4.00	1.00	4.00	2.00	2.00
46	3	5.00	5.00	4.00	4.00	4.00	4.00
47	2	5.00	4.00	4.00	5.00	4.00	4.00
48	3	5.00	4.00	4.00	4.00	4.00	4.00
49	2	5.00	4.00	4.00	5.00	4.00	4.00
50	2	5.00	5.00	4.00	4.00	5.00	3.00

	internet	vpn	عسكرية	إبراز	تجارية	تسلية	انتقام
1	5.00	4.00	1.00	5.00	2.00	5.00	5.00
2	5.00	4.00	2.00	3.00	4.00	4.00	5.00
3	5.00	4.00	2.00	3.00	4.00	4.00	5.00
4	5.00	2.00	2.00	3.00	4.00	4.00	5.00
5	4.00	1.00	1.00	2.00	1.00	3.00	1.00
6	5.00	2.00	1.00	5.00	2.00	5.00	5.00
7	5.00	2.00	1.00	5.00	2.00	5.00	5.00
8	5.00	2.00	1.00	5.00	2.00	5.00	5.00
9	5.00	2.00	2.00	4.00	4.00	4.00	5.00
10	5.00	3.00	1.00	5.00	2.00	5.00	5.00
11	5.00	3.00	1.00	5.00	2.00	5.00	5.00
12	5.00	4.00	2.00	3.00	4.00	4.00	5.00
13	5.00	2.00	2.00	3.00	4.00	4.00	5.00
14	5.00	2.00	1.00	5.00	2.00	5.00	5.00
15	5.00	2.00	1.00	5.00	2.00	5.00	5.00
16	5.00	4.00	2.00	5.00	4.00	4.00	5.00
17	5.00	4.00	1.00	5.00	2.00	5.00	5.00
18	5.00	4.00	2.00	3.00	4.00	4.00	5.00
19	5.00	4.00	1.00	5.00	2.00	5.00	5.00
20	5.00	4.00	2.00	5.00	4.00	4.00	5.00
21	2.00	1.00	1.00	4.00	1.00	3.00	1.00
22	2.00	1.00	1.00	4.00	1.00	3.00	1.00
23	5.00	4.00	1.00	5.00	2.00	5.00	5.00
24	5.00	4.00	1.00	5.00	2.00	5.00	5.00
25	5.00	4.00	2.00	3.00	4.00	4.00	5.00
26	5.00	4.00	1.00	5.00	2.00	5.00	5.00
27	5.00	4.00	2.00	3.00	4.00	4.00	5.00
28	5.00	4.00	1.00	5.00	2.00	5.00	5.00
29	5.00	4.00	2.00	3.00	4.00	4.00	5.00
30	5.00	4.00	2.00	3.00	4.00	4.00	5.00
31	5.00	4.00	2.00	5.00	5.00	4.00	5.00
32	5.00	4.00	2.00	3.00	4.00	4.00	5.00
33	5.00	4.00	2.00	3.00	4.00	4.00	5.00
34	2.00	1.00	1.00	5.00	3.00	5.00	5.00
35	5.00	4.00	1.00	5.00	2.00	5.00	5.00
36	2.00	1.00	1.00	4.00	2.00	3.00	4.00
37	4.00	1.00	1.00	4.00	5.00	1.00	4.00
38	2.00	1.00	1.00	5.00	5.00	3.00	3.00
39	4.00	1.00	1.00	4.00	5.00	3.00	4.00
40	4.00	1.00	1.00	4.00	5.00	3.00	1.00
41	4.00	2.00	1.00	4.00	5.00	3.00	1.00
42	2.00	1.00	1.00	5.00	3.00	1.00	3.00
43	5.00	1.00	1.00	4.00	4.00	3.00	1.00
44	3.00	1.00	1.00	4.00	4.00	3.00	2.00
45	4.00	1.00	1.00	4.00	4.00	3.00	2.00
46	5.00	2.00	1.00	5.00	4.00	5.00	4.00
47	5.00	4.00	1.00	5.00	2.00	5.00	4.00
48	5.00	2.00	1.00	5.00	4.00	5.00	3.00
49	5.00	3.00	1.00	5.00	2.00	5.00	4.00
50	5.00	3.00	1.00	5.00	2.00	5.00	4.00

	الشخصية	التكلفة	الإنذرات	الضعف	فيروس	طروادة	spoofing
1	5.00	2.00	2.00	4.000	5.00	5.00	4.00
2	4.00	2.00	4.00	5.000	5.00	4.00	5.00
3	5.00	2.00	4.00	5.000	5.00	4.00	3.00
4	5.00	2.00	2.00	5.000	5.00	4.00	3.00
5	4.00	1.00	1.00	2.000	3.00	5.00	2.00
6	3.00	3.00	2.00	4.000	5.00	5.00	4.00
7	3.00	2.00	2.00	4.000	5.00	5.00	4.00
8	5.00	2.00	2.00	4.000	5.00	5.00	4.00
9	5.00	4.00	2.00	5.000	5.00	4.00	3.00
10	4.00	2.00	3.00	4.000	5.00	5.00	4.00
11	3.00	2.00	2.00	4.000	5.00	5.00	4.00
12	3.00	2.00	3.00	5.000	5.00	4.00	3.00
13	5.00	4.00	3.00	5.000	5.00	4.00	5.00
14	2.00	3.00	3.00	4.000	5.00	5.00	4.00
15	4.00	3.00	2.00	4.000	5.00	5.00	4.00
16	3.00	3.00	2.00	5.000	5.00	4.00	3.00
17	4.00	1.00	2.00	4.000	5.00	5.00	4.00
18	5.00	1.00	.	5.000	5.00	4.00	3.00
19	4.00	2.00	.	4.000	5.00	5.00	5.00
20	5.00	3.00	3.00	5.000	5.00	4.00	3.00
21	4.00	1.00	.	2.000	3.00	2.00	5.00
22	3.00	1.00	.	2.000	3.00	2.00	4.00
23	5.00	2.00	5.00	4.000	5.00	5.00	4.00
24	5.00	2.00	5.00	4.000	5.00	5.00	5.00
25	5.00	3.00	6.00	5.000	5.00	4.00	5.00
26	5.00	2.00	2.00	4.000	5.00	5.00	4.00
27	2.00	3.00	2.00	5.000	5.00	4.00	5.00
28	5.00	3.00	.	4.000	5.00	5.00	4.00
29	4.00	4.00	.	5.000	5.00	4.00	5.00
30	5.00	5.00	.	5.000	5.00	4.00	4.00
31	5.00	3.00	.	5.000	5.00	4.00	3.00
32	4.00	3.00	.	5.000	5.00	5.00	4.00
33	4.00	2.00	1.00	5.000	5.00	4.00	4.00
34	4.00	1.00	1.00	2.000	3.00	5.00	5.00
35	4.00	2.00	2.00	4.000	5.00	5.00	4.00
36	4.00	1.00	1.00	2.000	3.00	2.00	3.00
37	4.00	2.00	1.00	1.000	2.00	2.00	2.00
38	3.00	1.00	1.00	2.000	3.00	4.00	2.00
39	2.00	1.00	3.00	2.000	3.00	3.00	4.00
40	4.00	1.00	1.00	2.000	3.00	2.00	2.00
41	4.00	1.00	1.00	2.000	3.00	2.00	2.00
42	3.00	1.00	.	1.000	2.00	2.00	4.00
43	4.00	1.00	1.00	2.000	3.00	4.00	2.00
44	4.00	1.00	.	2.000	3.00	3.00	4.00
45	4.00	1.00	1.00	2.000	3.00	2.00	2.00
46	5.00	2.00	.	4.000	5.00	5.00	4.00
47	5.00	1.00	.	4.000	5.00	5.00	4.00
48	5.00	2.00	.	4.000	5.00	5.00	4.00
49	5.00	2.00	.	4.000	5.00	5.00	4.00
50	5.00	1.00	.	4.000	5.00	5.00	4.00

	انتحال	المنافذ	التشارك	الثغرات	ثغراتتح	برمجة	إرفاق
1	4.00	4.00	5.00	5.00	4.00	4.00	3.00
2	3.00	5.00	5.00	5.00	5.00	4.00	4.00
3	3.00	5.00	5.00	5.00	5.00	4.00	4.00
4	3.00	5.00	5.00	5.00	5.00	4.00	4.00
5	1.00	2.00	1.00	1.00	2.00	1.00	1.00
6	4.00	4.00	5.00	5.00	4.00	4.00	3.00
7	4.00	4.00	5.00	5.00	4.00	4.00	3.00
8	4.00	4.00	5.00	5.00	4.00	4.00	3.00
9	3.00	5.00	5.00	5.00	5.00	4.00	4.00
10	4.00	4.00	5.00	5.00	4.00	4.00	3.00
11	4.00	4.00	5.00	5.00	4.00	4.00	3.00
12	3.00	5.00	5.00	5.00	5.00	4.00	4.00
13	3.00	5.00	5.00	5.00	5.00	4.00	4.00
14	4.00	4.00	5.00	5.00	4.00	4.00	3.00
15	4.00	4.00	5.00	5.00	4.00	4.00	3.00
16	3.00	5.00	5.00	5.00	5.00	4.00	4.00
17	4.00	4.00	5.00	5.00	4.00	4.00	3.00
18	3.00	5.00	5.00	5.00	5.00	4.00	4.00
19	4.00	4.00	5.00	5.00	4.00	4.00	3.00
20	3.00	5.00	5.00	5.00	5.00	4.00	4.00
21	1.00	2.00	1.00	1.00	2.00	1.00	1.00
22	1.00	2.00	1.00	1.00	2.00	1.00	1.00
23	4.00	4.00	5.00	5.00	4.00	4.00	3.00
24	4.00	4.00	5.00	5.00	4.00	4.00	3.00
25	3.00	5.00	5.00	5.00	5.00	4.00	4.00
26	4.00	4.00	5.00	5.00	4.00	4.00	3.00
27	3.00	5.00	5.00	5.00	5.00	4.00	4.00
28	4.00	4.00	5.00	5.00	4.00	4.00	3.00
29	3.00	5.00	5.00	5.00	5.00	4.00	4.00
30	3.00	5.00	5.00	5.00	5.00	4.00	4.00
31	3.00	5.00	5.00	5.00	5.00	4.00	4.00
32	3.00	5.00	5.00	5.00	5.00	4.00	4.00
33	3.00	5.00	5.00	5.00	5.00	4.00	4.00
34	1.00	2.00	1.00	1.00	2.00	1.00	1.00
35	4.00	4.00	5.00	5.00	4.00	4.00	3.00
36	1.00	2.00	1.00	1.00	2.00	1.00	1.00
37	1.00	2.00	1.00	2.00	1.00	1.00	2.00
38	1.00	4.00	4.00	1.00	2.00	1.00	1.00
39	1.00	4.00	4.00	2.00	2.00	1.00	1.00
40	1.00	2.00	1.00	2.00	2.00	1.00	1.00
41	1.00	2.00	1.00	1.00	2.00	1.00	1.00
42	1.00	4.00	5.00	1.00	1.00	1.00	2.00
43	3.00	2.00	4.00	1.00	2.00	1.00	1.00
44	1.00	4.00	1.00	1.00	2.00	1.00	1.00
45	3.00	2.00	1.00	2.00	2.00	1.00	1.00
46	4.00	4.00	5.00	5.00	4.00	4.00	3.00
47	4.00	2.00	5.00	5.00	4.00	4.00	3.00
48	4.00	4.00	5.00	5.00	4.00	4.00	3.00
49	4.00	4.00	5.00	5.00	4.00	4.00	3.00
50	4.00	4.00	5.00	5.00	4.00	4.00	3.00

	التخفي	المزودات	السرقة	تشغيل	ترك	زراعة	القانوني
1	4.00	5.00	5.00	3.00	4.00	2.00	4.00
2	3.00	5.00	5.00	3.00	3.00	3.00	4.00
3	3.00	5.00	3.00	3.00	3.00	3.00	4.00
4	3.00	5.00	3.00	3.00	3.00	3.00	5.00
5	2.00	1.00	5.00	1.00	3.00	1.00	5.00
6	4.00	5.00	4.00	3.00	4.00	2.00	4.00
7	4.00	5.00	5.00	3.00	4.00	2.00	4.00
8	4.00	5.00	5.00	3.00	4.00	2.00	4.00
9	3.00	5.00	3.00	3.00	2.00	3.00	5.00
10	4.00	5.00	5.00	3.00	4.00	2.00	4.00
11	4.00	5.00	5.00	3.00	2.00	2.00	4.00
12	3.00	5.00	3.00	3.00	5.00	3.00	2.00
13	3.00	5.00	3.00	3.00	2.00	3.00	2.00
14	4.00	5.00	5.00	3.00	4.00	2.00	4.00
15	4.00	5.00	5.00	3.00	4.00	4.00	4.00
16	3.00	5.00	3.00	3.00	3.00	3.00	3.00
17	4.00	5.00	5.00	3.00	4.00	2.00	4.00
18	3.00	5.00	3.00	3.00	3.00	3.00	2.00
19	4.00	5.00	5.00	3.00	3.00	2.00	4.00
20	3.00	5.00	3.00	3.00	3.00	3.00	2.00
21	2.00	3.00	1.00	1.00	3.00	1.00	4.00
22	2.00	4.00	1.00	1.00	3.00	1.00	3.00
23	4.00	5.00	5.00	3.00	4.00	2.00	4.00
24	4.00	5.00	5.00	3.00	4.00	2.00	4.00
25	3.00	5.00	3.00	3.00	3.00	3.00	2.00
26	4.00	5.00	5.00	3.00	3.00	2.00	4.00
27	3.00	5.00	3.00	3.00	3.00	3.00	2.00
28	4.00	5.00	5.00	3.00	3.00	2.00	4.00
29	3.00	5.00	3.00	3.00	5.00	3.00	2.00
30	3.00	5.00	3.00	3.00	5.00	3.00	2.00
31	3.00	5.00	3.00	3.00	3.00	3.00	2.00
32	3.00	5.00	3.00	3.00	3.00	3.00	2.00
33	3.00	5.00	3.00	3.00	3.00	3.00	2.00
34	2.00	1.00	1.00	1.00	3.00	1.00	1.00
35	4.00	5.00	5.00	3.00	4.00	2.00	4.00
36	2.00	1.00	1.00	1.00	3.00	1.00	1.00
37	1.00	1.00	1.00	1.00	4.00	1.00	4.00
38	2.00	1.00	1.00	1.00	3.00	1.00	4.00
39	2.00	1.00	1.00	1.00	3.00	1.00	1.00
40	2.00	1.00	1.00	1.00	3.00	1.00	1.00
41	2.00	1.00	1.00	1.00	3.00	1.00	1.00
42	1.00	1.00	1.00	1.00	4.00	1.00	1.00
43	2.00	1.00	1.00	1.00	3.00	1.00	3.00
44	2.00	1.00	1.00	1.00	3.00	1.00	1.00
45	2.00	1.00	1.00	1.00	3.00	1.00	3.00
46	4.00	5.00	5.00	3.00	4.00	2.00	4.00
47	4.00	5.00	5.00	3.00	4.00	2.00	4.00
48	4.00	5.00	5.00	3.00	4.00	2.00	4.00
49	4.00	5.00	5.00	3.00	4.00	2.00	4.00
50	4.00	5.00	5.00	3.00	3.00	2.00	4.00

	الصيانة	مرخص	غمرخص	مجاني	غمجاني	cookies	groove
1	2.00	3.00	5.00	5.00	4.00	5.00	3.00
2	4.00	4.00	5.00	5.00	4.00	5.00	4.00
3	3.00	3.00	5.00	5.00	4.00	5.00	4.00
4	4.00	4.00	5.00	5.00	4.00	5.00	4.00
5	1.00	1.00	4.00	5.00	3.00	4.00	2.00
6	3.00	3.00	5.00	5.00	4.00	5.00	3.00
7	3.00	3.00	5.00	5.00	4.00	5.00	3.00
8	3.00	1.00	5.00	5.00	4.00	5.00	3.00
9	3.00	3.00	5.00	5.00	4.00	5.00	1.00
10	3.00	3.00	5.00	5.00	4.00	5.00	3.00
11	3.00	3.00	5.00	5.00	4.00	5.00	3.00
12	3.00	3.00	5.00	5.00	4.00	5.00	4.00
13	3.00	3.00	5.00	5.00	4.00	5.00	4.00
14	3.00	3.00	5.00	5.00	4.00	5.00	3.00
15	2.00	3.00	5.00	5.00	4.00	5.00	3.00
16	3.00	4.00	5.00	5.00	4.00	5.00	4.00
17	3.00	3.00	5.00	5.00	4.00	5.00	3.00
18	3.00	3.00	5.00	5.00	4.00	5.00	4.00
19	3.00	3.00	5.00	5.00	4.00	5.00	3.00
20	3.00	4.00	5.00	5.00	3.00	5.00	4.00
21	1.00	1.00	4.00	5.00	3.00	4.00	2.00
22	2.00	1.00	4.00	5.00	3.00	4.00	2.00
23	3.00	3.00	5.00	4.00	4.00	5.00	3.00
24	3.00	3.00	5.00	5.00	4.00	5.00	3.00
25	3.00	4.00	5.00	5.00	4.00	5.00	4.00
26	3.00	3.00	5.00	5.00	4.00	5.00	3.00
27	3.00	4.00	5.00	5.00	4.00	5.00	4.00
28	3.00	3.00	5.00	5.00	4.00	5.00	3.00
29	2.00	4.00	5.00	5.00	4.00	5.00	4.00
30	3.00	4.00	5.00	5.00	4.00	5.00	4.00
31	4.00	3.00	5.00	5.00	4.00	5.00	4.00
32	3.00	4.00	5.00	5.00	4.00	5.00	4.00
33	3.00	4.00	5.00	5.00	4.00	5.00	4.00
34	4.00	1.00	4.00	5.00	3.00	4.00	2.00
35	4.00	3.00	5.00	5.00	4.00	5.00	3.00
36	3.00	1.00	4.00	5.00	3.00	4.00	2.00
37	2.00	2.00	5.00	5.00	4.00	3.00	1.00
38	1.00	1.00	4.00	5.00	3.00	4.00	2.00
39	1.00	1.00	4.00	5.00	3.00	4.00	2.00
40	3.00	1.00	4.00	5.00	3.00	4.00	2.00
41	1.00	1.00	4.00	5.00	3.00	4.00	2.00
42	4.00	2.00	5.00	5.00	4.00	3.00	2.00
43	1.00	1.00	4.00	5.00	3.00	4.00	2.00
44	1.00	1.00	4.00	5.00	3.00	4.00	3.00
45	4.00	1.00	4.00	5.00	3.00	4.00	2.00
46	3.00	3.00	5.00	5.00	4.00	5.00	3.00
47	3.00	3.00	5.00	5.00	4.00	5.00	1.00
48	3.00	3.00	5.00	5.00	4.00	5.00	3.00
49	3.00	3.00	5.00	5.00	4.00	5.00	2.00
50	3.00	3.00	5.00	5.00	4.00	5.00	1.00

	caligula	netbus	subseven	hack	wincrash	tfn	toolkit
1	3.00	4.00	4.00	5.00	4.00	2.00	4.00
2	4.00	5.00	5.00	4.00	3.00	3.00	5.00
3	4.00	5.00	5.00	4.00	3.00	5.00	5.00
4	4.00	5.00	5.00	4.00	3.00	5.00	5.00
5	2.00	2.00	2.00	2.00	3.00	5.00	2.00
6	3.00	4.00	4.00	3.00	4.00	4.00	4.00
7	3.00	4.00	4.00	5.00	4.00	5.00	4.00
8	3.00	4.00	4.00	3.00	4.00	4.00	4.00
9	1.00	5.00	5.00	4.00	3.00	5.00	5.00
10	3.00	4.00	4.00	5.00	4.00	5.00	4.00
11	3.00	4.00	4.00	3.00	4.00	5.00	4.00
12	4.00	5.00	5.00	4.00	3.00	5.00	5.00
13	4.00	5.00	5.00	4.00	4.00	5.00	3.00
14	3.00	4.00	4.00	3.00	4.00	5.00	4.00
15	3.00	4.00	4.00	3.00	4.00	5.00	4.00
16	4.00	5.00	5.00	4.00	3.00	3.00	5.00
17	3.00	4.00	4.00	5.00	4.00	2.00	4.00
18	4.00	5.00	5.00	4.00	3.00	3.00	3.00
19	3.00	4.00	4.00	5.00	4.00	2.00	4.00
20	4.00	5.00	5.00	4.00	3.00	3.00	3.00
21	2.00	5.00	4.00	2.00	2.00	5.00	2.00
22	2.00	5.00	4.00	2.00	2.00	5.00	2.00
23	3.00	4.00	4.00	5.00	5.00	5.00	4.00
24	3.00	4.00	4.00	5.00	5.00	5.00	4.00
25	4.00	5.00	5.00	4.00	3.00	3.00	3.00
26	3.00	4.00	4.00	5.00	4.00	2.00	4.00
27	4.00	5.00	5.00	4.00	3.00	3.00	5.00
28	3.00	4.00	4.00	5.00	4.00	2.00	4.00
29	4.00	5.00	5.00	4.00	3.00	3.00	3.00
30	4.00	5.00	5.00	4.00	3.00	3.00	5.00
31	4.00	5.00	5.00	4.00	3.00	3.00	5.00
32	4.00	5.00	5.00	4.00	3.00	3.00	3.00
33	4.00	5.00	5.00	4.00	3.00	3.00	4.00
34	2.00	2.00	2.00	2.00	2.00	2.00	2.00
35	3.00	4.00	4.00	3.00	4.00	2.00	4.00
36	2.00	2.00	2.00	2.00	2.00	2.00	2.00
37	2.00	2.00	2.00	2.00	2.00	3.00	2.00
38	2.00	2.00	2.00	2.00	2.00	2.00	2.00
39	2.00	2.00	2.00	2.00	2.00	4.00	2.00
40	2.00	2.00	2.00	2.00	2.00	2.00	3.00
41	2.00	2.00	2.00	2.00	2.00	5.00	2.00
42	2.00	3.00	3.00	2.00	2.00	3.00	2.00
43	2.00	4.00	2.00	2.00	2.00	2.00	3.00
44	3.00	4.00	4.00	3.00	3.00	2.00	2.00
45	2.00	2.00	2.00	2.00	2.00	4.00	2.00
46	1.00	4.00	4.00	4.00	5.00	4.00	4.00
47	3.00	4.00	4.00	3.00	4.00	4.00	4.00
48	1.00	1.00	1.00	3.00	5.00	4.00	3.00
49	2.00	4.00	4.00	1.00	4.00	4.00	4.00
50	3.00	4.00	4.00	2.00	4.00	3.00	4.00

	msword	msexcel	revelat	icq	بتنصت	بالتغيل	المشاركة
1	4.00	4.00	3.00	3.00	3.00	3.00	5.00
2	4.00	4.00	2.00	5.00	4.00	4.00	4.00
3	4.00	4.00	4.00	5.00	4.00	4.00	4.00
4	4.00	4.00	4.00	5.00	4.00	2.00	4.00
5	2.00	2.00	2.00	4.00	3.00	3.00	3.00
6	3.00	3.00	3.00	3.00	3.00	2.00	5.00
7	3.00	3.00	3.00	3.00	5.00	3.00	5.00
8	3.00	3.00	3.00	3.00	5.00	3.00	5.00
9	3.00	3.00	3.00	5.00	5.00	3.00	4.00
10	4.00	4.00	3.00	5.00	5.00	3.00	5.00
11	3.00	3.00	2.00	4.00	5.00	3.00	5.00
12	3.00	3.00	2.00	5.00	4.00	2.00	4.00
13	3.00	4.00	4.00	5.00	4.00	2.00	4.00
14	3.00	4.00	2.00	3.00	3.00	3.00	5.00
15	3.00	3.00	2.00	3.00	5.00	3.00	5.00
16	3.00	3.00	2.00	5.00	5.00	3.00	4.00
17	3.00	3.00	2.00	3.00	5.00	3.00	5.00
18	3.00	3.00	2.00	5.00	5.00	3.00	4.00
19	3.00	3.00	3.00	3.00	5.00	3.00	5.00
20	4.00	4.00	4.00	5.00	5.00	4.00	4.00
21	2.00	2.00	2.00	2.00	3.00	3.00	3.00
22	2.00	2.00	2.00	2.00	3.00	3.00	3.00
23	5.00	3.00	3.00	3.00	3.00	3.00	5.00
24	3.00	3.00	3.00	3.00	3.00	3.00	5.00
25	3.00	3.00	2.00	5.00	4.00	4.00	4.00
26	3.00	3.00	2.00	3.00	3.00	3.00	5.00
27	5.00	3.00	2.00	5.00	4.00	4.00	4.00
28	3.00	3.00	3.00	3.00	3.00	3.00	5.00
29	3.00	4.00	2.00	5.00	4.00	4.00	4.00
30	3.00	3.00	2.00	5.00	4.00	4.00	4.00
31	3.00	3.00	2.00	5.00	4.00	4.00	4.00
32	3.00	3.00	2.00	5.00	4.00	4.00	4.00
33	3.00	3.00	2.00	5.00	4.00	4.00	4.00
34	2.00	2.00	2.00	5.00	5.00	3.00	5.00
35	5.00	5.00	3.00	3.00	3.00	3.00	5.00
36	2.00	2.00	2.00	3.00	3.00	3.00	3.00
37	2.00	2.00	2.00	3.00	2.00	2.00	2.00
38	2.00	2.00	2.00	3.00	3.00	3.00	3.00
39	2.00	3.00	2.00	3.00	3.00	3.00	3.00
40	3.00	3.00	2.00	2.00	3.00	3.00	3.00
41	2.00	2.00	2.00	4.00	3.00	3.00	3.00
42	2.00	2.00	2.00	2.00	3.00	2.00	2.00
43	2.00	2.00	2.00	3.00	3.00	2.00	3.00
44	2.00	2.00	2.00	2.00	5.00	3.00	5.00
45	2.00	3.00	2.00	2.00	3.00	2.00	3.00
46	3.00	3.00	3.00	3.00	3.00	2.00	5.00
47	3.00	3.00	3.00	3.00	5.00	3.00	5.00
48	3.00	3.00	3.00	3.00	5.00	3.00	5.00
49	3.00	3.00	3.00	3.00	5.00	2.00	5.00
50	2.00	2.00	3.00	3.00	5.00	3.00	5.00

	البريد	الديدان	التقنية	الحمايةت	تكلفةلتو	تكلفةستخ	مصدر
1	5.00	5.00	4.00	5.00	5.00	5.00	4.00
2	4.00	5.00	5.00	4.00	4.00	3.00	3.00
3	4.00	5.00	5.00	4.00	4.00	3.00	3.00
4	4.00	5.00	5.00	4.00	4.00	3.00	3.00
5	4.00	3.00	5.00	5.00	4.00	4.00	4.00
6	5.00	5.00	4.00	5.00	5.00	5.00	4.00
7	5.00	5.00	4.00	5.00	5.00	5.00	4.00
8	5.00	5.00	4.00	5.00	5.00	5.00	4.00
9	5.00	5.00	5.00	4.00	4.00	3.00	3.00
10	5.00	5.00	4.00	5.00	5.00	5.00	4.00
11	5.00	5.00	4.00	5.00	5.00	5.00	4.00
12	3.00	5.00	5.00	4.00	4.00	3.00	3.00
13	3.00	5.00	5.00	4.00	4.00	3.00	3.00
14	5.00	5.00	4.00	5.00	5.00	5.00	4.00
15	5.00	5.00	4.00	5.00	5.00	5.00	4.00
16	5.00	5.00	5.00	4.00	4.00	3.00	3.00
17	5.00	5.00	4.00	5.00	5.00	5.00	4.00
18	5.00	5.00	5.00	4.00	4.00	3.00	3.00
19	5.00	5.00	4.00	5.00	5.00	5.00	4.00
20	5.00	5.00	5.00	4.00	4.00	3.00	3.00
21	5.00	3.00	5.00	5.00	4.00	4.00	4.00
22	5.00	3.00	5.00	5.00	4.00	4.00	4.00
23	5.00	5.00	4.00	5.00	5.00	5.00	4.00
24	5.00	5.00	4.00	5.00	5.00	5.00	4.00
25	3.00	5.00	5.00	4.00	4.00	3.00	3.00
26	5.00	5.00	4.00	5.00	5.00	5.00	4.00
27	3.00	5.00	5.00	4.00	4.00	3.00	3.00
28	5.00	5.00	4.00	5.00	5.00	5.00	4.00
29	3.00	5.00	5.00	4.00	4.00	3.00	3.00
30	3.00	5.00	5.00	4.00	4.00	3.00	3.00
31	3.00	5.00	5.00	4.00	4.00	3.00	3.00
32	3.00	5.00	5.00	4.00	4.00	3.00	3.00
33	3.00	5.00	5.00	4.00	4.00	3.00	3.00
34	5.00	5.00	5.00	5.00	4.00	4.00	4.00
35	5.00	5.00	4.00	5.00	5.00	5.00	4.00
36	5.00	5.00	4.00	4.00	4.00	3.00	4.00
37	5.00	5.00	4.00	3.00	4.00	3.00	4.00
38	5.00	5.00	5.00	5.00	4.00	4.00	4.00
39	5.00	5.00	5.00	5.00	4.00	4.00	4.00
40	5.00	5.00	4.00	4.00	4.00	3.00	4.00
41	3.00	3.00	4.00	4.00	4.00	3.00	4.00
42	3.00	3.00	4.00	3.00	4.00	3.00	4.00
43	3.00	3.00	4.00	4.00	4.00	3.00	4.00
44	5.00	4.00	5.00	5.00	4.00	4.00	4.00
45	3.00	3.00	5.00	5.00	4.00	4.00	4.00
46	5.00	5.00	4.00	5.00	5.00	5.00	4.00
47	5.00	5.00	4.00	5.00	5.00	5.00	4.00
48	5.00	5.00	4.00	5.00	5.00	5.00	4.00
49	5.00	5.00	4.00	5.00	5.00	5.00	4.00
50	5.00	5.00	4.00	5.00	5.00	5.00	4.00

	var00001	ip	حمايةتتع	ضبط	دليل	الديبي	الد
1	4.00	5.00	5.00	3.00	.	.	.
2	3.00	6.00	5.00	3.00	.	.	.
3	3.00	6.00	7.00	3.00	.	.	.
4	3.00	7.00	7.00	3.00	.	.	.
5	4.00	7.00	6.00	1.00	.	.	.
6	4.00	5.00	7.00	1.00	.	.	.
7	3.00	6.00	5.00	1.00	.	.	.
8	2.00	7.00	6.00	3.00	.	.	.
9	3.00	5.00	6.00	3.00	.	.	.
10	2.00	6.00	6.00	3.00	.	.	.
11	4.00	6.00	7.00	3.00	.	.	.
12	3.00	7.00	6.00	3.00	.	.	.
13	3.00	6.00	6.00	1.00	.	.	.
14	2.00	7.00	6.00	1.00	.	.	.
15	3.00	7.00	6.00	3.00	.	.	.
16	3.00	7.00	6.00	3.00	.	.	.
17	3.00	7.00	6.00	3.00	.	.	.
18	3.00	6.00	6.00	3.00	.	.	.
19	3.00	6.00	6.00	3.00	.	.	.
20	2.00	7.00	6.00	3.00	.	.	.
21	3.00	7.00	7.00	3.00	.	.	.
22	4.00	5.00	6.00	3.00	.	.	.
23	4.00	6.00	5.00	3.00	.	.	.
24	4.00	7.00	6.00	3.00	.	.	.
25	3.00	5.00	6.00	3.00	.	.	.
26	2.00	6.00	6.00	3.00	.	.	.
27	2.00	6.00	6.00	3.00	.	.	.
28	2.00	7.00	6.00	3.00	.	.	.
29	2.00	6.00	6.00	3.00	.	.	.
30	2.00	7.00	7.00	3.00	.	.	.
31	2.00	6.00	6.00	3.00	.	.	.
32	3.00	7.00	6.00	3.00	.	.	.
33	3.00	7.00	6.00	3.00	.	.	.
34	4.00	5.00	6.00	3.00	.	.	.
35	4.00	6.00	5.00	1.00	.	.	.
36	3.00	7.00	6.00	1.00	.	.	.
37	3.00	5.00	7.00	1.00	.	.	.
38	3.00	6.00	6.00	1.00	.	.	.
39	4.00	6.00	7.00	1.00	.	.	.
40	3.00	7.00	6.00	3.00	.	.	.
41	3.00	6.00	6.00	3.00	.	.	.
42	4.00	7.00	6.00	3.00	.	.	.
43	3.00	7.00	6.00	3.00	.	.	.
44	3.00	7.00	6.00	3.00	.	.	.
45	2.00	7.00	7.00	1.00	.	.	.
46	3.00	7.00	6.00	3.00	.	.	.
47	3.00	7.00	6.00	3.00	.	.	.
48	4.00	7.00	6.00	3.00	.	.	.
49	3.00	7.00	7.00	3.00	.	.	.
50	4.00	7.00	7.00	3.00	.	.	.

	var00005	البلاغ	كفاءة	الخوف	الرغبة	اكتشاف	محدودية
1	.	5.00	4.00	4.00	4.00	3.00	4.00
2	.	5.00	4.00	5.00	4.00	4.00	4.00
3	.	5.00	4.00	5.00	4.00	4.00	4.00
4	.	4.00	4.00	5.00	4.00	4.00	4.00
5	.	5.00	1.00	5.00	5.00	1.00	4.00
6	.	5.00	4.00	4.00	4.00	3.00	4.00
7	.	5.00	4.00	4.00	4.00	4.00	4.00
8	.	5.00	4.00	4.00	4.00	4.00	4.00
9	.	5.00	4.00	5.00	5.00	4.00	5.00
10	.	5.00	4.00	5.00	5.00	4.00	5.00
11	.	5.00	4.00	5.00	5.00	4.00	4.00
12	.	5.00	4.00	5.00	5.00	4.00	5.00
13	.	5.00	4.00	5.00	5.00	4.00	5.00
14	.	5.00	4.00	4.00	4.00	3.00	4.00
15	.	5.00	4.00	4.00	4.00	3.00	4.00
16	.	5.00	4.00	5.00	5.00	4.00	4.00
17	.	5.00	4.00	4.00	4.00	3.00	4.00
18	.	5.00	4.00	5.00	4.00	4.00	4.00
19	.	5.00	4.00	4.00	4.00	3.00	4.00
20	.	5.00	4.00	5.00	3.00	4.00	3.00
21	.	5.00	1.00	4.00	4.00	4.00	4.00
22	.	5.00	1.00	4.00	4.00	4.00	4.00
23	.	5.00	4.00	4.00	4.00	3.00	4.00
24	.	5.00	4.00	4.00	4.00	3.00	4.00
25	.	5.00	4.00	5.00	5.00	4.00	4.00
26	.	5.00	4.00	5.00	5.00	3.00	4.00
27	.	5.00	4.00	5.00	5.00	4.00	4.00
28	.	5.00	4.00	4.00	4.00	3.00	4.00
29	.	5.00	4.00	5.00	5.00	4.00	5.00
30	.	5.00	4.00	5.00	4.00	4.00	4.00
31	.	5.00	4.00	5.00	5.00	4.00	5.00
32	.	5.00	4.00	5.00	4.00	4.00	4.00
33	.	5.00	4.00	3.00	3.00	4.00	3.00
34	.	5.00	1.00	4.00	4.00	1.00	4.00
35	.	5.00	4.00	4.00	4.00	3.00	4.00
36	.	5.00	1.00	4.00	4.00	4.00	4.00
37	.	5.00	1.00	4.00	4.00	4.00	1.00
38	.	5.00	1.00	4.00	4.00	4.00	4.00
39	.	5.00	1.00	4.00	4.00	4.00	1.00
40	.	5.00	1.00	3.00	3.00	4.00	3.00
41	.	5.00	1.00	3.00	3.00	2.00	3.00
42	.	5.00	1.00	3.00	3.00	2.00	3.00
43	.	5.00	1.00	4.00	4.00	2.00	4.00
44	.	5.00	1.00	3.00	3.00	2.00	3.00
45	.	5.00	1.00	3.00	3.00	2.00	3.00
46	.	5.00	4.00	5.00	5.00	3.00	5.00
47	.	5.00	4.00	4.00	4.00	3.00	4.00
48	.	5.00	2.00	4.00	4.00	4.00	4.00
49	.	5.00	2.00	4.00	4.00	3.00	4.00
50	.	5.00	2.00	4.00	4.00	3.00	4.00

	التشفير	سجل	auditing	مراقبة	الشبكة	report	مراجعة
1	4.00	5.00	5.00	5.00	4.00	5.00	4.00
2	4.00	5.00	4.00	4.00	5.00	5.00	3.00
3	4.00	5.00	4.00	4.00	5.00	5.00	3.00
4	4.00	5.00	4.00	4.00	5.00	5.00	3.00
5	5.00	5.00	5.00	5.00	4.00	5.00	5.00
6	4.00	5.00	5.00	5.00	4.00	5.00	4.00
7	4.00	5.00	5.00	5.00	4.00	5.00	4.00
8	4.00	5.00	5.00	5.00	4.00	5.00	4.00
9	4.00	5.00	4.00	4.00	4.00	5.00	3.00
10	4.00	5.00	5.00	5.00	4.00	5.00	4.00
11	4.00	5.00	5.00	5.00	4.00	5.00	4.00
12	4.00	5.00	4.00	4.00	5.00	5.00	3.00
13	4.00	5.00	4.00	4.00	5.00	5.00	3.00
14	3.00	5.00	5.00	5.00	4.00	5.00	4.00
15	2.00	5.00	5.00	5.00	4.00	5.00	4.00
16	2.00	5.00	4.00	4.00	5.00	5.00	3.00
17	2.00	5.00	5.00	5.00	4.00	5.00	4.00
18	2.00	5.00	4.00	4.00	5.00	5.00	3.00
19	3.00	5.00	5.00	5.00	4.00	5.00	4.00
20	2.00	5.00	4.00	3.00	5.00	5.00	3.00
21	5.00	5.00	5.00	5.00	4.00	5.00	5.00
22	5.00	5.00	5.00	5.00	4.00	5.00	5.00
23	4.00	5.00	5.00	5.00	4.00	5.00	4.00
24	4.00	5.00	5.00	5.00	4.00	5.00	4.00
25	4.00	5.00	4.00	4.00	5.00	5.00	3.00
26	3.00	5.00	5.00	5.00	4.00	5.00	4.00
27	4.00	5.00	4.00	4.00	5.00	5.00	3.00
28	4.00	5.00	5.00	5.00	4.00	5.00	4.00
29	4.00	5.00	4.00	4.00	5.00	5.00	3.00
30	4.00	5.00	4.00	4.00	5.00	5.00	3.00
31	4.00	5.00	4.00	4.00	5.00	5.00	3.00
32	4.00	5.00	4.00	4.00	5.00	5.00	3.00
33	4.00	5.00	4.00	4.00	5.00	5.00	3.00
34	2.00	5.00	5.00	5.00	4.00	5.00	5.00
35	4.00	5.00	5.00	5.00	4.00	5.00	4.00
36	2.00	5.00	5.00	5.00	4.00	4.00	4.00
37	2.00	5.00	4.00	4.00	3.00	5.00	4.00
38	2.00	5.00	5.00	5.00	4.00	5.00	5.00
39	5.00	5.00	5.00	5.00	4.00	5.00	5.00
40	5.00	5.00	5.00	5.00	4.00	4.00	4.00
41	2.00	5.00	5.00	5.00	4.00	4.00	4.00
42	2.00	5.00	4.00	4.00	3.00	5.00	4.00
43	5.00	5.00	5.00	5.00	4.00	4.00	4.00
44	5.00	5.00	5.00	5.00	4.00	5.00	5.00
45	5.00	5.00	5.00	5.00	4.00	5.00	5.00
46	3.00	5.00	5.00	5.00	4.00	5.00	4.00
47	4.00	5.00	5.00	5.00	4.00	5.00	4.00
48	4.00	5.00	5.00	5.00	4.00	5.00	4.00
49	4.00	5.00	5.00	5.00	4.00	5.00	4.00
50	4.00	5.00	5.00	3.00	4.00	5.00	4.00

	الجدران	تتبعمختر	تتبعمصدر	كسر	كشف	viewdisk	pkzip
1	5.00	3.00	3.00	3.00	5.00	5.00	4.00
2	4.00	5.00	5.00	5.00	5.00	3.00	3.00
3	4.00	5.00	5.00	5.00	5.00	3.00	3.00
4	4.00	5.00	5.00	5.00	4.00	3.00	3.00
5	5.00	4.00	4.00	5.00	4.00	3.00	3.00
6	5.00	3.00	2.00	3.00	4.00	5.00	4.00
7	5.00	3.00	3.00	3.00	4.00	5.00	4.00
8	5.00	3.00	3.00	3.00	5.00	5.00	4.00
9	4.00	5.00	5.00	5.00	4.00	3.00	3.00
10	5.00	3.00	3.00	3.00	5.00	5.00	4.00
11	5.00	3.00	3.00	3.00	5.00	5.00	4.00
12	4.00	5.00	5.00	5.00	5.00	3.00	3.00
13	4.00	5.00	2.00	5.00	4.00	3.00	3.00
14	5.00	3.00	3.00	3.00	5.00	5.00	4.00
15	5.00	3.00	2.00	3.00	5.00	5.00	4.00
16	4.00	5.00	5.00	5.00	5.00	3.00	3.00
17	5.00	3.00	3.00	3.00	4.00	5.00	4.00
18	4.00	5.00	5.00	5.00	4.00	3.00	3.00
19	5.00	3.00	3.00	3.00	5.00	5.00	4.00
20	4.00	5.00	2.00	5.00	5.00	3.00	3.00
21	5.00	4.00	4.00	5.00	5.00	3.00	3.00
22	5.00	4.00	4.00	5.00	5.00	3.00	3.00
23	5.00	3.00	3.00	3.00	5.00	5.00	4.00
24	5.00	3.00	3.00	3.00	4.00	5.00	4.00
25	4.00	5.00	5.00	5.00	5.00	3.00	3.00
26	5.00	3.00	3.00	3.00	5.00	5.00	4.00
27	4.00	5.00	5.00	5.00	5.00	3.00	3.00
28	5.00	3.00	3.00	3.00	5.00	5.00	4.00
29	4.00	5.00	5.00	5.00	5.00	3.00	3.00
30	4.00	5.00	5.00	5.00	5.00	3.00	3.00
31	4.00	5.00	5.00	5.00	5.00	3.00	3.00
32	4.00	5.00	5.00	5.00	5.00	3.00	3.00
33	4.00	5.00	5.00	5.00	5.00	3.00	3.00
34	5.00	4.00	4.00	5.00	5.00	3.00	3.00
35	5.00	3.00	3.00	3.00	5.00	5.00	4.00
36	4.00	4.00	4.00	3.00	5.00	3.00	3.00
37	4.00	4.00	4.00	3.00	5.00	3.00	2.00
38	5.00	4.00	4.00	5.00	5.00	3.00	3.00
39	5.00	4.00	4.00	5.00	5.00	3.00	3.00
40	4.00	4.00	4.00	3.00	5.00	3.00	3.00
41	4.00	4.00	4.00	3.00	5.00	3.00	3.00
42	4.00	4.00	4.00	3.00	5.00	3.00	2.00
43	4.00	4.00	4.00	3.00	5.00	3.00	3.00
44	5.00	4.00	4.00	5.00	4.00	3.00	3.00
45	5.00	4.00	4.00	5.00	4.00	3.00	3.00
46	5.00	4.00	4.00	3.00	5.00	5.00	1.00
47	5.00	3.00	3.00	3.00	5.00	5.00	1.00
48	5.00	3.00	3.00	3.00	5.00	5.00	1.00
49	5.00	4.00	2.00	3.00	5.00	5.00	1.00
50	5.00	3.00	3.00	3.00	4.00	5.00	1.00

	xtreepro	lantast	diskette	laplink	المقارنة	logging	تشريعات
1	3.00	2.00	3.00	3.00	4.00	5.00	5.00
2	3.00	3.00	4.00	4.00	4.00	5.00	5.00
3	3.00	3.00	4.00	4.00	4.00	5.00	5.00
4	3.00	3.00	4.00	4.00	4.00	5.00	5.00
5	4.00	1.00	3.00	4.00	3.00	5.00	4.00
6	3.00	1.00	3.00	3.00	4.00	5.00	5.00
7	3.00	1.00	3.00	3.00	4.00	5.00	5.00
8	3.00	1.00	3.00	3.00	4.00	5.00	5.00
9	3.00	1.00	4.00	4.00	4.00	4.00	5.00
10	3.00	2.00	3.00	3.00	4.00	5.00	5.00
11	3.00	2.00	3.00	3.00	4.00	5.00	5.00
12	3.00	3.00	4.00	4.00	4.00	5.00	5.00
13	3.00	3.00	4.00	4.00	4.00	5.00	5.00
14	3.00	2.00	3.00	3.00	4.00	5.00	5.00
15	2.00	1.00	3.00	4.00	4.00	5.00	5.00
16	2.00	1.00	4.00	4.00	4.00	4.00	5.00
17	2.00	1.00	3.00	3.00	4.00	5.00	5.00
18	2.00	1.00	4.00	4.00	4.00	4.00	5.00
19	2.00	1.00	3.00	3.00	4.00	5.00	5.00
20	3.00	1.00	4.00	4.00	4.00	4.00	5.00
21	4.00	2.00	3.00	2.00	3.00	5.00	4.00
22	4.00	2.00	3.00	4.00	3.00	5.00	4.00
23	3.00	2.00	3.00	3.00	4.00	5.00	5.00
24	3.00	2.00	3.00	3.00	4.00	5.00	5.00
25	3.00	3.00	4.00	3.00	4.00	4.00	5.00
26	3.00	2.00	3.00	3.00	4.00	5.00	5.00
27	3.00	3.00	4.00	3.00	4.00	4.00	5.00
28	2.00	3.00	3.00	3.00	4.00	5.00	5.00
29	2.00	2.00	4.00	3.00	4.00	4.00	5.00
30	2.00	2.00	4.00	3.00	4.00	4.00	5.00
31	2.00	2.00	4.00	3.00	4.00	4.00	5.00
32	2.00	2.00	4.00	3.00	4.00	4.00	5.00
33	2.00	2.00	4.00	3.00	4.00	4.00	5.00
34	4.00	2.00	3.00	3.00	3.00	5.00	4.00
35	3.00	2.00	3.00	3.00	4.00	5.00	5.00
36	4.00	2.00	3.00	3.00	3.00	5.00	4.00
37	4.00	3.00	3.00	3.00	3.00	4.00	3.00
38	4.00	2.00	3.00	3.00	3.00	5.00	4.00
39	4.00	2.00	3.00	2.00	3.00	5.00	4.00
40	4.00	2.00	3.00	2.00	3.00	5.00	4.00
41	4.00	2.00	3.00	2.00	3.00	5.00	4.00
42	2.00	3.00	3.00	3.00	3.00	4.00	3.00
43	4.00	2.00	3.00	2.00	3.00	5.00	4.00
44	3.00	2.00	3.00	2.00	2.00	5.00	4.00
45	4.00	2.00	3.00	2.00	3.00	5.00	4.00
46	3.00	2.00	4.00	3.00	2.00	5.00	5.00
47	3.00	1.00	3.00	3.00	4.00	5.00	5.00
48	3.00	2.00	3.00	3.00	2.00	5.00	5.00
49	3.00	2.00	3.00	3.00	4.00	5.00	5.00
50	3.00	2.00	4.00	3.00	4.00	5.00	5.00

	مكونات	متخصص	التحقيق	مستجدات	تحديث	قناعة	الشكوى
1	4.00	3.00	5.00	3.00	2.00	1.00	5.00
2	4.00	2.00	2.00	3.00	4.00	4.00	3.00
3	4.00	2.00	2.00	3.00	4.00	4.00	3.00
4	4.00	2.00	2.00	3.00	4.00	4.00	3.00
5	3.00	2.00	5.00	3.00	4.00	3.00	4.00
6	4.00	3.00	5.00	3.00	2.00	1.00	5.00
7	4.00	3.00	5.00	3.00	2.00	1.00	5.00
8	4.00	3.00	5.00	3.00	2.00	1.00	5.00
9	4.00	2.00	2.00	3.00	4.00	4.00	3.00
10	4.00	3.00	5.00	3.00	2.00	1.00	5.00
11	4.00	3.00	5.00	3.00	2.00	1.00	5.00
12	4.00	2.00	2.00	3.00	4.00	4.00	3.00
13	4.00	2.00	2.00	3.00	4.00	4.00	3.00
14	4.00	3.00	5.00	3.00	2.00	1.00	5.00
15	4.00	3.00	5.00	3.00	2.00	1.00	5.00
16	4.00	2.00	2.00	3.00	4.00	4.00	3.00
17	4.00	3.00	5.00	3.00	2.00	1.00	5.00
18	4.00	2.00	2.00	3.00	4.00	4.00	3.00
19	4.00	3.00	5.00	3.00	2.00	1.00	5.00
20	4.00	2.00	2.00	3.00	4.00	4.00	3.00
21	3.00	2.00	5.00	3.00	4.00	3.00	4.00
22	3.00	2.00	5.00	3.00	4.00	3.00	4.00
23	4.00	3.00	5.00	3.00	2.00	1.00	5.00
24	4.00	3.00	5.00	3.00	2.00	1.00	5.00
25	4.00	2.00	2.00	3.00	4.00	4.00	3.00
26	4.00	3.00	5.00	3.00	2.00	1.00	5.00
27	4.00	2.00	2.00	3.00	4.00	4.00	3.00
28	4.00	3.00	5.00	3.00	2.00	1.00	5.00
29	4.00	2.00	2.00	3.00	4.00	4.00	3.00
30	4.00	2.00	2.00	3.00	4.00	4.00	3.00
31	4.00	2.00	2.00	3.00	4.00	4.00	3.00
32	4.00	2.00	2.00	3.00	4.00	4.00	3.00
33	4.00	2.00	2.00	3.00	4.00	4.00	3.00
34	3.00	2.00	5.00	3.00	4.00	3.00	4.00
35	4.00	3.00	5.00	3.00	2.00	1.00	5.00
36	3.00	2.00	5.00	3.00	4.00	3.00	4.00
37	3.00	2.00	2.00	2.00	2.00	4.00	3.00
38	3.00	2.00	5.00	3.00	4.00	3.00	4.00
39	3.00	2.00	5.00	3.00	4.00	3.00	4.00
40	3.00	2.00	5.00	3.00	4.00	3.00	4.00
41	3.00	2.00	5.00	3.00	4.00	3.00	4.00
42	3.00	2.00	2.00	2.00	2.00	4.00	3.00
43	3.00	2.00	5.00	3.00	4.00	3.00	4.00
44	3.00	2.00	5.00	3.00	4.00	3.00	4.00
45	3.00	2.00	5.00	3.00	4.00	3.00	4.00
46	4.00	3.00	5.00	3.00	2.00	1.00	5.00
47	4.00	3.00	5.00	3.00	2.00	1.00	5.00
48	4.00	3.00	5.00	3.00	2.00	1.00	5.00
49	4.00	3.00	5.00	3.00	2.00	1.00	5.00
50	4.00	3.00	5.00	3.00	2.00	1.00	5.00

	يقاوم	تناسب	التدريب	الخبراء	تصميم	عنبعد	تنسيقاً
1	4.00	3.00	3.00	1.00	1.00	1.00	3.00
2	3.00	4.00	4.00	2.00	2.00	2.00	3.00
3	3.00	4.00	4.00	2.00	2.00	2.00	3.00
4	3.00	4.00	4.00	2.00	2.00	2.00	3.00
5	4.00	3.00	4.00	3.00	2.00	2.00	1.00
6	4.00	3.00	3.00	1.00	1.00	1.00	3.00
7	4.00	3.00	3.00	1.00	1.00	1.00	3.00
8	4.00	3.00	3.00	1.00	1.00	1.00	2.00
9	3.00	4.00	4.00	2.00	2.00	2.00	2.00
10	4.00	3.00	3.00	1.00	1.00	1.00	2.00
11	4.00	3.00	3.00	1.00	1.00	1.00	2.00
12	3.00	4.00	4.00	2.00	2.00	2.00	2.00
13	3.00	4.00	4.00	2.00	2.00	2.00	2.00
14	4.00	3.00	3.00	1.00	1.00	1.00	2.00
15	4.00	3.00	3.00	1.00	1.00	1.00	3.00
16	3.00	4.00	4.00	2.00	2.00	2.00	2.00
17	4.00	3.00	3.00	1.00	1.00	1.00	2.00
18	3.00	4.00	4.00	2.00	2.00	2.00	2.00
19	4.00	3.00	3.00	1.00	1.00	1.00	2.00
20	3.00	4.00	4.00	2.00	2.00	2.00	3.00
21	4.00	3.00	4.00	3.00	2.00	2.00	1.00
22	4.00	3.00	4.00	3.00	2.00	2.00	1.00
23	4.00	3.00	3.00	1.00	1.00	1.00	2.00
24	4.00	3.00	3.00	1.00	1.00	1.00	2.00
25	3.00	4.00	4.00	2.00	2.00	2.00	2.00
26	4.00	3.00	3.00	1.00	1.00	1.00	2.00
27	3.00	4.00	4.00	2.00	2.00	2.00	2.00
28	4.00	3.00	3.00	1.00	1.00	1.00	2.00
29	3.00	4.00	4.00	2.00	2.00	2.00	2.00
30	3.00	4.00	4.00	2.00	2.00	2.00	3.00
31	3.00	4.00	4.00	2.00	2.00	2.00	3.00
32	3.00	4.00	4.00	2.00	2.00	2.00	2.00
33	3.00	4.00	4.00	2.00	2.00	2.00	2.00
34	4.00	3.00	4.00	3.00	2.00	2.00	2.00
35	4.00	3.00	3.00	1.00	1.00	1.00	2.00
36	4.00	3.00	4.00	3.00	2.00	2.00	1.00
37	4.00	2.00	2.00	2.00	4.00	2.00	1.00
38	4.00	3.00	4.00	3.00	2.00	2.00	1.00
39	4.00	3.00	4.00	3.00	2.00	2.00	1.00
40	4.00	3.00	4.00	3.00	2.00	2.00	1.00
41	4.00	3.00	4.00	3.00	2.00	2.00	1.00
42	4.00	2.00	2.00	2.00	4.00	2.00	1.00
43	4.00	3.00	4.00	3.00	2.00	2.00	1.00
44	4.00	3.00	4.00	3.00	3.00	2.00	1.00
45	4.00	3.00	4.00	3.00	2.00	2.00	1.00
46	4.00	3.00	3.00	1.00	1.00	1.00	3.00
47	4.00	3.00	3.00	1.00	1.00	1.00	2.00
48	4.00	3.00	3.00	1.00	1.00	1.00	2.00
49	4.00	3.00	3.00	1.00	3.00	1.00	2.00
50	4.00	3.00	3.00	1.00	1.00	1.00	2.00

	تنسيقنم	مناسب	المختصين	معاهد	اهمية	التوعية	أشتراك
1	3.00	.	.	.	5.00	5.00	1
2	3.00	.	.	.	5.00	2.00	1
3	3.00	.	.	.	5.00	2.00	1
4	3.00	.	.	.	5.00	2.00	1
5	3.00	.	.	.	5.00	4.00	1
6	3.00	.	.	.	5.00	5.00	1
7	3.00	.	.	.	5.00	5.00	1
8	3.00	.	.	.	5.00	5.00	1
9	3.00	.	.	.	5.00	2.00	1
10	3.00	.	.	.	5.00	5.00	1
11	3.00	.	.	.	5.00	5.00	1
12	3.00	.	.	.	5.00	2.00	1
13	3.00	.	.	.	5.00	2.00	1
14	3.00	.	.	.	5.00	5.00	1
15	3.00	.	.	.	5.00	5.00	1
16	3.00	.	.	.	5.00	2.00	1
17	3.00	.	.	.	5.00	5.00	1
18	3.00	.	.	.	5.00	2.00	1
19	3.00	.	.	.	5.00	5.00	1
20	3.00	.	.	.	5.00	2.00	1
21	3.00	.	.	.	5.00	4.00	2
22	3.00	.	.	.	5.00	4.00	1
23	3.00	.	.	.	5.00	5.00	2
24	3.00	.	.	.	5.00	5.00	1
25	3.00	.	.	.	5.00	2.00	2
26	3.00	.	.	.	5.00	5.00	2
27	3.00	.	.	.	5.00	2.00	1
28	3.00	.	.	.	5.00	5.00	1
29	3.00	.	.	.	5.00	2.00	1
30	3.00	.	.	.	5.00	2.00	1
31	3.00	.	.	.	5.00	2.00	1
32	3.00	.	.	.	5.00	1.00	1
33	3.00	.	.	.	5.00	2.00	1
34	3.00	.	.	.	5.00	4.00	1
35	3.00	.	.	.	5.00	5.00	1
36	3.00	.	.	.	5.00	2.00	1
37	4.00	.	.	.	5.00	6.00	1
38	3.00	.	.	.	5.00	1.00	2
39	3.00	.	.	.	5.00	4.00	1
40	3.00	.	.	.	5.00	1.00	2
41	3.00	.	.	.	5.00	1.00	1
42	4.00	.	.	.	5.00	6.00	1
43	3.00	.	.	.	5.00	2.00	1
44	3.00	.	.	.	5.00	2.00	1
45	3.00	.	.	.	5.00	2.00	1
46	3.00	.	.	.	5.00	5.00	1
47	3.00	.	.	.	4.00	1.00	2
48	3.00	.	.	.	4.00	1.00	2
49	3.00	.	.	.	5.00	5.00	1
50	3.00	.	.	.	5.00	5.00	1

	المهارة	المعرفة	المقدرة	بأساليب	الإثبات	الدوري	الزام
1	.	.	.	.	.	5.00	4.00
2	.	.	.	.	.	4.00	3.00
3	.	.	.	.	.	4.00	3.00
4	.	.	.	.	.	4.00	3.00
5	.	.	.	.	.	3.00	4.00
6	.	.	.	.	.	5.00	4.00
7	.	.	.	.	.	5.00	4.00
8	.	.	.	.	.	5.00	4.00
9	.	.	.	.	.	4.00	3.00
10	.	.	.	.	.	5.00	4.00
11	.	.	.	.	.	5.00	4.00
12	.	.	.	.	.	4.00	3.00
13	.	.	.	.	.	4.00	3.00
14	.	.	.	.	.	5.00	4.00
15	.	.	.	.	.	5.00	4.00
16	.	.	.	.	.	4.00	3.00
17	.	.	.	.	.	5.00	4.00
18	.	.	.	.	.	4.00	3.00
19	.	.	.	.	.	5.00	4.00
20	.	.	.	.	.	4.00	3.00
21	.	.	.	.	.	3.00	4.00
22	.	.	.	.	.	3.00	4.00
23	.	.	.	.	.	5.00	4.00
24	.	.	.	.	.	5.00	4.00
25	.	.	.	.	.	4.00	3.00
26	.	.	.	.	.	5.00	4.00
27	.	.	.	.	.	4.00	3.00
28	.	.	.	.	.	5.00	4.00
29	.	.	.	.	.	4.00	3.00
30	.	.	.	.	.	4.00	3.00
31	.	.	.	.	.	4.00	3.00
32	.	.	.	.	.	4.00	3.00
33	.	.	.	.	.	4.00	3.00
34	.	.	.	.	.	3.00	4.00
35	.	.	.	.	.	5.00	4.00
36	.	.	.	.	.	1.00	5.00
37	.	.	.	.	.	5.00	4.00
38	.	.	.	.	.	3.00	4.00
39	.	.	.	.	.	3.00	4.00
40	.	.	.	.	.	1.00	5.00
41	.	.	.	.	.	1.00	5.00
42	.	.	.	.	.	5.00	4.00
43	.	.	.	.	.	1.00	5.00
44	.	.	.	.	.	3.00	4.00
45	.	.	.	.	.	3.00	4.00
46	.	.	.	.	.	1.00	4.00
47	.	.	.	.	.	1.00	4.00
48	.	.	.	.	.	2.00	4.00
49	.	.	.	.	.	1.00	4.00
50	.	.	.	.	.	2.00	3.00

	الحوافز	توزيع	التزكية	المصرح	بصمة	محركات	لصيانة
1	5.00	4.00	4.00	4.00	5.00	1.00	3.00
2	2.00	4.00	3.00	4.00	4.00	3.00	3.00
3	2.00	4.00	3.00	4.00	4.00	3.00	3.00
4	2.00	4.00	3.00	4.00	4.00	3.00	3.00
5	2.00	4.00	4.00	4.00	1.00	3.00	5.00
6	2.00	4.00	4.00	4.00	5.00	1.00	3.00
7	5.00	4.00	4.00	4.00	5.00	1.00	3.00
8	5.00	4.00	4.00	4.00	5.00	1.00	3.00
9	2.00	4.00	3.00	4.00	4.00	3.00	3.00
10	1.00	4.00	4.00	4.00	5.00	1.00	3.00
11	5.00	4.00	4.00	4.00	5.00	1.00	3.00
12	2.00	4.00	3.00	4.00	4.00	3.00	3.00
13	2.00	4.00	3.00	4.00	4.00	3.00	3.00
14	3.00	4.00	4.00	4.00	5.00	1.00	3.00
15	5.00	4.00	4.00	4.00	5.00	1.00	3.00
16	2.00	4.00	3.00	4.00	4.00	3.00	3.00
17	5.00	4.00	4.00	4.00	5.00	1.00	3.00
18	2.00	4.00	3.00	4.00	4.00	3.00	3.00
19	3.00	4.00	4.00	4.00	5.00	1.00	3.00
20	3.00	4.00	3.00	4.00	4.00	3.00	3.00
21	2.00	4.00	4.00	4.00	1.00	3.00	5.00
22	2.00	4.00	4.00	4.00	1.00	3.00	5.00
23	2.00	4.00	4.00	4.00	5.00	1.00	3.00
24	1.00	4.00	4.00	4.00	5.00	1.00	3.00
25	2.00	4.00	3.00	4.00	4.00	3.00	3.00
26	2.00	4.00	4.00	4.00	5.00	1.00	3.00
27	2.00	4.00	3.00	4.00	4.00	3.00	3.00
28	5.00	4.00	4.00	4.00	5.00	1.00	3.00
29	1.00	4.00	3.00	4.00	4.00	3.00	3.00
30	2.00	4.00	3.00	4.00	4.00	3.00	3.00
31	2.00	4.00	3.00	4.00	4.00	3.00	3.00
32	2.00	4.00	3.00	4.00	4.00	3.00	3.00
33	2.00	4.00	3.00	4.00	4.00	3.00	3.00
34	2.00	4.00	4.00	4.00	1.00	3.00	5.00
35	5.00	4.00	4.00	4.00	5.00	1.00	3.00
36	1.00	4.00	4.00	4.00	1.00	3.00	5.00
37	3.00	4.00	5.00	4.00	4.00	4.00	4.00
38	2.00	4.00	4.00	4.00	1.00	3.00	5.00
39	2.00	4.00	4.00	4.00	1.00	3.00	5.00
40	1.00	4.00	4.00	4.00	1.00	3.00	5.00
41	1.00	4.00	4.00	4.00	1.00	3.00	5.00
42	3.00	4.00	5.00	4.00	3.00	4.00	4.00
43	1.00	4.00	4.00	4.00	1.00	3.00	5.00
44	2.00	4.00	4.00	4.00	1.00	3.00	5.00
45	2.00	4.00	4.00	4.00	1.00	3.00	5.00
46	3.00	4.00	4.00	4.00	3.00	1.00	3.00
47	1.00	4.00	4.00	4.00	1.00	1.00	3.00
48	1.00	4.00	4.00	4.00	2.00	1.00	3.00
49	1.00	4.00	4.00	4.00	1.00	1.00	3.00
50	2.00	4.00	4.00	4.00	1.00	1.00	3.00

	الأحتياط	تحديثها	المدة	المزامنة	تلائم	باستمرار	التقدم
1	3.00	2.00	2.00	1.00	5.00	5.00	4.00
2	3.00	2.00	2.00	2.00	4.00	4.00	3.00
3	3.00	2.00	2.00	2.00	4.00	4.00	3.00
4	3.00	2.00	2.00	2.00	4.00	4.00	3.00
5	5.00	5.00	4.00	5.00	4.00	4.00	4.00
6	3.00	2.00	2.00	1.00	5.00	5.00	4.00
7	3.00	4.00	2.00	1.00	5.00	5.00	4.00
8	3.00	2.00	2.00	1.00	5.00	4.00	2.00
9	3.00	3.00	2.00	2.00	4.00	4.00	3.00
10	3.00	2.00	2.00	1.00	5.00	5.00	4.00
11	3.00	2.00	2.00	1.00	5.00	5.00	4.00
12	3.00	2.00	2.00	2.00	4.00	4.00	3.00
13	3.00	3.00	2.00	2.00	4.00	4.00	3.00
14	3.00	2.00	2.00	1.00	5.00	5.00	4.00
15	3.00	4.00	2.00	1.00	5.00	5.00	4.00
16	3.00	2.00	2.00	2.00	4.00	4.00	3.00
17	3.00	2.00	2.00	1.00	5.00	5.00	4.00
18	3.00	2.00	2.00	2.00	4.00	4.00	3.00
19	3.00	2.00	2.00	1.00	5.00	5.00	4.00
20	3.00	2.00	2.00	2.00	4.00	4.00	3.00
21	5.00	3.00	4.00	3.00	4.00	4.00	3.00
22	5.00	5.00	4.00	3.00	4.00	4.00	2.00
23	3.00	2.00	2.00	1.00	5.00	5.00	3.00
24	3.00	2.00	2.00	1.00	5.00	5.00	4.00
25	3.00	2.00	2.00	2.00	4.00	4.00	3.00
26	3.00	2.00	2.00	1.00	5.00	5.00	4.00
27	3.00	2.00	2.00	2.00	4.00	4.00	3.00
28	3.00	2.00	2.00	1.00	5.00	5.00	2.00
29	3.00	2.00	2.00	2.00	4.00	4.00	3.00
30	3.00	2.00	2.00	2.00	4.00	4.00	3.00
31	3.00	2.00	2.00	2.00	4.00	4.00	3.00
32	3.00	4.00	2.00	2.00	4.00	4.00	3.00
33	3.00	2.00	2.00	2.00	4.00	4.00	3.00
34	5.00	5.00	4.00	5.00	4.00	4.00	4.00
35	3.00	2.00	2.00	1.00	5.00	5.00	2.00
36	5.00	5.00	4.00	5.00	4.00	1.00	3.00
37	4.00	5.00	4.00	3.00	4.00	1.00	3.00
38	5.00	5.00	4.00	4.00	4.00	4.00	2.00
39	5.00	5.00	4.00	4.00	4.00	4.00	2.00
40	5.00	5.00	4.00	2.00	4.00	3.00	3.00
41	5.00	5.00	4.00	4.00	4.00	3.00	3.00
42	4.00	4.00	4.00	3.00	4.00	4.00	3.00
43	5.00	5.00	4.00	1.00	4.00	4.00	3.00
44	5.00	4.00	4.00	4.00	4.00	1.00	4.00
45	5.00	5.00	4.00	2.00	4.00	1.00	4.00
46	3.00	2.00	2.00	3.00	5.00	1.00	2.00
47	3.00	2.00	2.00	3.00	5.00	1.00	2.00
48	3.00	2.00	2.00	2.00	5.00	1.00	2.00
49	3.00	2.00	1.00	3.00	5.00	1.00	2.00
50	3.00	2.00	3.00	2.00	5.00	1.00	2.00

	تشكيل	رصد	التتبع	ربط	ضوابطتشغ	ضوابطعمل	ظوابطقاع
1	5.00	5.00	5.00	5.00	4.00	3.00	4.00
2	4.00	4.00	3.00	4.00	4.00	3.00	3.00
3	4.00	4.00	3.00	4.00	4.00	3.00	3.00
4	4.00	4.00	3.00	4.00	4.00	3.00	3.00
5	4.00	4.00	4.00	4.00	4.00	4.00	4.00
6	5.00	5.00	5.00	5.00	4.00	3.00	4.00
7	4.00	5.00	5.00	2.00	4.00	3.00	4.00
8	4.00	5.00	5.00	2.00	4.00	3.00	4.00
9	4.00	4.00	3.00	3.00	4.00	3.00	3.00
10	5.00	5.00	5.00	5.00	4.00	3.00	4.00
11	4.00	5.00	5.00	2.00	3.00	3.00	4.00
12	4.00	4.00	3.00	3.00	4.00	3.00	3.00
13	4.00	4.00	3.00	4.00	4.00	3.00	3.00
14	3.00	5.00	2.00	3.00	4.00	3.00	4.00
15	4.00	5.00	4.00	1.00	4.00	3.00	4.00
16	4.00	4.00	3.00	2.00	4.00	3.00	3.00
17	2.00	5.00	3.00	2.00	4.00	3.00	4.00
18	2.00	4.00	3.00	4.00	4.00	3.00	3.00
19	5.00	5.00	3.00	5.00	4.00	3.00	4.00
20	2.00	4.00	3.00	2.00	4.00	3.00	3.00
21	2.00	4.00	3.00	2.00	4.00	4.00	4.00
22	2.00	4.00	3.00	4.00	4.00	4.00	4.00
23	3.00	5.00	4.00	3.00	4.00	3.00	4.00
24	2.00	5.00	4.00	4.00	4.00	3.00	4.00
25	4.00	4.00	3.00	4.00	4.00	3.00	3.00
26	3.00	3.00	5.00	1.00	4.00	3.00	4.00
27	4.00	4.00	3.00	1.00	4.00	3.00	3.00
28	2.00	3.00	5.00	1.00	4.00	3.00	4.00
29	3.00	4.00	3.00	2.00	4.00	3.00	3.00
30	2.00	4.00	3.00	1.00	4.00	3.00	3.00
31	2.00	2.00	3.00	1.00	4.00	3.00	3.00
32	2.00	4.00	3.00	1.00	4.00	3.00	3.00
33	2.00	4.00	3.00	3.00	4.00	3.00	3.00
34	4.00	4.00	4.00	1.00	4.00	4.00	4.00
35	2.00	2.00	3.00	1.00	4.00	3.00	4.00
36	2.00	1.00	2.00	1.00	5.00	4.00	1.00
37	2.00	3.00	3.00	1.00	5.00	4.00	1.00
38	2.00	4.00	3.00	1.00	4.00	4.00	4.00
39	2.00	4.00	4.00	1.00	4.00	4.00	4.00
40	1.00	1.00	5.00	4.00	5.00	4.00	1.00
41	1.00	2.00	1.00	1.00	5.00	4.00	1.00
42	1.00	2.00	5.00	4.00	5.00	4.00	1.00
43	1.00	3.00	1.00	4.00	5.00	4.00	1.00
44	4.00	3.00	1.00	4.00	4.00	3.00	4.00
45	4.00	2.00	1.00	2.00	4.00	4.00	4.00
46	4.00	3.00	1.00	3.00	4.00	4.00	4.00
47	3.00	3.00	1.00	3.00	4.00	4.00	4.00
48	4.00	3.00	1.00	1.00	4.00	4.00	4.00
49	2.00	3.00	4.00	3.00	2.00	4.00	3.00
50	3.00	3.00	3.00	2.00	2.00	2.00	3.00

	ظوابطشبك	ضوابطالد	البشري	المكاني	المطورة	الجاهزة	الانترنت
1	3.00	3.00	4.00	5.00	4.00	5.00	4.00
2	4.00	3.00	4.00	5.00	3.00	5.00	5.00
3	4.00	3.00	4.00	5.00	3.00	5.00	5.00
4	4.00	3.00	4.00	5.00	3.00	5.00	5.00
5	4.00	4.00	5.00	5.00	5.00	5.00	5.00
6	3.00	3.00	4.00	5.00	4.00	5.00	4.00
7	3.00	3.00	4.00	4.00	4.00	5.00	4.00
8	3.00	3.00	4.00	5.00	4.00	5.00	4.00
9	4.00	3.00	4.00	5.00	3.00	5.00	5.00
10	3.00	3.00	4.00	5.00	4.00	5.00	4.00
11	3.00	3.00	4.00	5.00	4.00	5.00	4.00
12	4.00	3.00	4.00	5.00	3.00	5.00	5.00
13	4.00	3.00	4.00	5.00	3.00	5.00	5.00
14	3.00	3.00	4.00	5.00	4.00	5.00	4.00
15	3.00	3.00	4.00	5.00	4.00	5.00	4.00
16	4.00	3.00	4.00	5.00	3.00	5.00	5.00
17	3.00	3.00	4.00	5.00	4.00	5.00	4.00
18	4.00	3.00	4.00	5.00	3.00	5.00	5.00
19	3.00	3.00	4.00	5.00	4.00	5.00	4.00
20	4.00	3.00	4.00	5.00	3.00	5.00	5.00
21	4.00	4.00	5.00	5.00	5.00	5.00	5.00
22	4.00	4.00	5.00	5.00	5.00	5.00	5.00
23	3.00	3.00	4.00	5.00	4.00	5.00	4.00
24	3.00	3.00	4.00	5.00	4.00	5.00	4.00
25	4.00	3.00	4.00	5.00	3.00	5.00	5.00
26	3.00	3.00	4.00	5.00	4.00	5.00	4.00
27	4.00	3.00	4.00	5.00	3.00	5.00	5.00
28	3.00	3.00	4.00	5.00	4.00	5.00	4.00
29	4.00	3.00	4.00	5.00	3.00	5.00	5.00
30	4.00	3.00	4.00	5.00	3.00	5.00	5.00
31	4.00	3.00	4.00	5.00	3.00	5.00	5.00
32	4.00	3.00	4.00	5.00	3.00	5.00	5.00
33	4.00	3.00	4.00	4.00	3.00	5.00	5.00
34	4.00	4.00	5.00	5.00	5.00	5.00	5.00
35	3.00	3.00	4.00	5.00	4.00	5.00	4.00
36	3.00	5.00	5.00	5.00	4.00	5.00	4.00
37	3.00	5.00	5.00	5.00	4.00	5.00	4.00
38	4.00	4.00	5.00	5.00	5.00	5.00	5.00
39	4.00	4.00	5.00	5.00	5.00	5.00	5.00
40	3.00	5.00	5.00	5.00	4.00	5.00	4.00
41	3.00	5.00	5.00	5.00	4.00	5.00	4.00
42	3.00	5.00	5.00	5.00	4.00	5.00	4.00
43	3.00	4.00	5.00	5.00	4.00	5.00	4.00
44	4.00	4.00	5.00	4.00	5.00	5.00	5.00
45	4.00	4.00	5.00	5.00	5.00	5.00	5.00
46	2.00	4.00	4.00	3.00	4.00	5.00	4.00
47	1.00	4.00	4.00	3.00	4.00	5.00	4.00
48	2.00	4.00	4.00	3.00	4.00	4.00	4.00
49	2.00	4.00	4.00	5.00	4.00	4.00	4.00
50	2.00	4.00	4.00	3.00	4.00	5.00	4.00

	الخدمات	احترازات	وسائط	منافسين	السياسة	التشريعا	المجرمين
1	3.00	3.00	3.00	1.00	5.00	5.00	5.00
2	4.00	4.00	4.00	3.00	5.00	5.00	5.00
3	4.00	4.00	4.00	3.00	5.00	5.00	5.00
4	4.00	4.00	4.00	3.00	5.00	5.00	5.00
5	5.00	5.00	5.00	5.00	5.00	5.00	5.00
6	3.00	3.00	3.00	1.00	5.00	5.00	5.00
7	3.00	3.00	3.00	1.00	5.00	5.00	5.00
8	3.00	3.00	3.00	1.00	5.00	5.00	5.00
9	4.00	4.00	4.00	3.00	5.00	5.00	5.00
10	3.00	3.00	3.00	1.00	5.00	5.00	5.00
11	3.00	3.00	3.00	1.00	5.00	5.00	5.00
12	4.00	4.00	4.00	3.00	5.00	5.00	5.00
13	4.00	4.00	4.00	3.00	5.00	5.00	5.00
14	3.00	3.00	3.00	1.00	5.00	5.00	5.00
15	3.00	3.00	3.00	1.00	5.00	5.00	5.00
16	4.00	4.00	4.00	3.00	5.00	5.00	5.00
17	3.00	3.00	3.00	1.00	5.00	5.00	5.00
18	4.00	4.00	4.00	3.00	5.00	5.00	5.00
19	3.00	3.00	3.00	1.00	5.00	5.00	5.00
20	4.00	4.00	4.00	3.00	5.00	5.00	5.00
21	5.00	5.00	5.00	5.00	5.00	5.00	5.00
22	5.00	5.00	5.00	5.00	5.00	5.00	5.00
23	3.00	3.00	3.00	1.00	5.00	5.00	5.00
24	3.00	3.00	3.00	1.00	5.00	5.00	5.00
25	4.00	4.00	4.00	3.00	5.00	5.00	5.00
26	3.00	3.00	3.00	1.00	5.00	5.00	5.00
27	4.00	4.00	4.00	3.00	5.00	5.00	5.00
28	3.00	3.00	3.00	1.00	5.00	5.00	5.00
29	4.00	4.00	4.00	3.00	5.00	5.00	5.00
30	4.00	4.00	4.00	3.00	5.00	5.00	5.00
31	4.00	4.00	4.00	3.00	5.00	5.00	5.00
32	4.00	4.00	4.00	3.00	5.00	5.00	5.00
33	4.00	4.00	4.00	3.00	5.00	5.00	5.00
34	5.00	5.00	5.00	5.00	5.00	5.00	5.00
35	3.00	3.00	3.00	1.00	5.00	5.00	5.00
36	5.00	5.00	5.00	5.00	5.00	5.00	5.00
37	5.00	5.00	5.00	3.00	5.00	4.00	4.00
38	5.00	5.00	5.00	5.00	5.00	5.00	5.00
39	5.00	5.00	5.00	5.00	5.00	5.00	5.00
40	5.00	5.00	5.00	5.00	5.00	5.00	5.00
41	5.00	5.00	5.00	5.00	5.00	5.00	5.00
42	5.00	5.00	5.00	3.00	5.00	4.00	4.00
43	5.00	5.00	5.00	5.00	5.00	5.00	5.00
44	5.00	5.00	5.00	5.00	5.00	5.00	5.00
45	5.00	5.00	5.00	5.00	5.00	5.00	5.00
46	3.00	3.00	3.00	1.00	5.00	5.00	5.00
47	3.00	3.00	3.00	1.00	5.00	5.00	5.00
48	3.00	3.00	3.00	1.00	5.00	5.00	5.00
49	3.00	3.00	3.00	1.00	5.00	5.00	5.00
50	3.00	3.00	3.00	1.00	5.00	5.00	5.00

	الرؤساء	عقوبات	أعلان	lev_1	العينةz	zsc001	المطورةz
1	4.00	5.00	5.00	.05	-.93157	-.93157	-.05569
2	4.00	5.00	5.00	.09	-.93157	-.93157	-1.36437
3	4.00	5.00	5.00	.09	-.93157	-.93157	-1.36437
4	4.00	5.00	5.00	.09	-.93157	-.93157	-1.36437
5	5.00	5.00	5.00	.22	-.93157	-.93157	1.25299
6	4.00	5.00	5.00	.05	-.93157	-.93157	-.05569
7	4.00	5.00	5.00	.09	-.93157	-.93157	-.05569
8	4.00	5.00	5.00	.09	-.93157	-.93157	-.05569
9	4.00	5.00	5.00	.19	-.93157	-.93157	-1.36437
10	4.00	5.00	5.00	.17	-.93157	-.93157	-.05569
11	4.00	5.00	5.00	.05	-.93157	-.93157	-.05569
12	4.00	5.00	5.00	.10	-.93157	-.93157	-1.36437
13	4.00	5.00	5.00	.05	-.93157	-.93157	-1.36437
14	4.00	5.00	5.00	.16	-.93157	-.93157	-.05569
15	4.00	5.00	5.00	.15	-.93157	-.93157	-.05569
16	4.00	5.00	5.00	.07	-.93157	-.93157	-1.36437
17	4.00	5.00	5.00	.06	-.93157	-.93157	-.05569
18	4.00	5.00	5.00	.07	-.93157	-.93157	-1.36437
19	4.00	5.00	5.00	.14	-.93157	-.93157	-.05569
20	4.00	5.00	5.00	.05	-.93157	-.93157	-1.36437
21	5.00	5.00	5.00	.32	-.93157	-.93157	1.25299
22	5.00	5.00	5.00	.18	-.93157	-.93157	1.25299
23	4.00	5.00	5.00	.09	-.93157	-.93157	-.05569
24	4.00	5.00	4.00	.09	-.93157	-.93157	-.05569
25	4.00	5.00	5.00	.09	-.93157	-.93157	-1.36437
26	4.00	5.00	5.00	.10	-.93157	-.93157	-.05569
27	4.00	5.00	5.00	.09	-.93157	-.93157	-1.36437
28	4.00	5.00	5.00	.09	-.93157	-.93157	-.05569
29	4.00	5.00	5.00	.11	-.93157	-.93157	-1.36437
30	4.00	5.00	5.00	.11	-.93157	-.93157	-1.36437
31	4.00	5.00	5.00	.06	-.93157	-.93157	-1.36437
32	4.00	5.00	4.00	.07	-.93157	-.93157	-1.36437
33	4.00	5.00	4.00	.06	-.93157	-.93157	-1.36437
34	5.00	5.00	4.00	.27	-.93157	-.93157	1.25299
35	4.00	5.00	4.00	.07	-.93157	-.93157	-.05569
36	5.00	5.00	4.00	.37	-.93157	-.93157	-.05569
37	5.00	4.00	5.00	.18	-.93157	-.93157	-.05569
38	5.00	5.00	5.00	.23	-.93157	-.93157	1.25299
39	5.00	5.00	5.00	.36	-.93157	-.93157	1.25299
40	5.00	5.00	4.00	.32	-.93157	-.93157	-.05569
41	5.00	5.00	4.00	.23	-.93157	-.93157	-.05569
42	5.00	4.00	5.00	.14	-.93157	-.93157	-.05569
43	5.00	5.00	2.00	.20	-.93157	-.93157	-.05569
44	5.00	5.00	5.00	.13	-.93157	-.93157	1.25299
45	5.00	5.00	5.00	.14	-.93157	-.93157	1.25299
46	4.00	5.00	5.00	.36	-.93157	-.93157	-.05569
47	4.00	5.00	5.00	.60	-.93157	-.93157	-.05569
48	4.00	5.00	2.00	.42	-.93157	-.93157	-.05569
49	4.00	5.00	4.00	.12	-.93157	-.93157	-.05569
50	4.00	5.00	4.00	.28	-.93157	-.93157	-.05569

	الجاهزةz	الانترنz	الخدماتz	احترازاz	وسائطz	منافسينz
1	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
2	.72622	.83704	.17560	.24176	.05569	-.17476
3	.72622	.83704	.17560	.24176	.05569	-.17476
4	.72622	.83704	.17560	.24176	.05569	-.17476
5	.72622	.83704	1.47876	1.50430	1.36437	1.19422
6	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
7	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
8	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
9	.72622	.83704	.17560	.24176	.05569	-.17476
10	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
11	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
12	.72622	.83704	.17560	.24176	.05569	-.17476
13	.72622	.83704	.17560	.24176	.05569	-.17476
14	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
15	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
16	.72622	.83704	.17560	.24176	.05569	-.17476
17	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
18	.72622	.83704	.17560	.24176	.05569	-.17476
19	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
20	.72622	.83704	.17560	.24176	.05569	-.17476
21	.72622	.83704	1.47876	1.50430	1.36437	1.19422
22	.72622	.83704	1.47876	1.50430	1.36437	1.19422
23	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
24	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
25	.72622	.83704	.17560	.24176	.05569	-.17476
26	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
27	.72622	.83704	.17560	.24176	.05569	-.17476
28	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
29	.72622	.83704	.17560	.24176	.05569	-.17476
30	.72622	.83704	.17560	.24176	.05569	-.17476
31	.72622	.83704	.17560	.24176	.05569	-.17476
32	.72622	.83704	.17560	.24176	.05569	-.17476
33	.72622	.83704	.17560	.24176	.05569	-.17476
34	.72622	.83704	1.47876	1.50430	1.36437	1.19422
35	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
36	.72622	-.84900	1.47876	1.50430	1.36437	1.19422
37	.72622	-.84900	1.47876	1.50430	1.36437	-.17476
38	.72622	.83704	1.47876	1.50430	1.36437	1.19422
39	.72622	.83704	1.47876	1.50430	1.36437	1.19422
40	.72622	-.84900	1.47876	1.50430	1.36437	1.19422
41	.72622	-.84900	1.47876	1.50430	1.36437	1.19422
42	.72622	-.84900	1.47876	1.50430	1.36437	-.17476
43	.72622	-.84900	1.47876	1.50430	1.36437	1.19422
44	.72622	.83704	1.47876	1.50430	1.36437	1.19422
45	.72622	.83704	1.47876	1.50430	1.36437	1.19422
46	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
47	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
48	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
49	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
50	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374

	العينة	الوظيفة	المؤسسة	v3	الأنترنت	الاسلوب	مصروفات
51	1.00	3.00	4.00	2.00	2.00	2	1
52	1.00	1.00	4.00	1.00	3.00	4	1
53	1.00	1.00	4.00	1.00	2.00	1	1
54	1.00	3.00	4.00	2.00	2.00	3	1
55	1.00	1.00	4.00	1.00	2.00	1	1
56	1.00	3.00	4.00	1.00	2.00	2	1
57	1.00	3.00	4.00	3.00	1.00	3	1
58	1.00	2.00	2.00	2.00	1.00	2	3
59	1.00	3.00	2.00	3.00	1.00	2	2
60	1.00	1.00	2.00	3.00	2.00	2	2
61	1.00	6.00	2.00	3.00	2.00	2	3
62	1.00	9.00	2.00	3.00	1.00	2	2
63	1.00	7.00	2.00	3.00	1.00	2	2
64	1.00	8.00	2.00	3.00	1.00	2	3
65	1.00	6.00	2.00	3.00	1.00	2	3
66	1.00	6.00	2.00	3.00	1.00	2	3
67	1.00	8.00	2.00	3.00	1.00	2	2
68	1.00	8.00	2.00	2.00	1.00	2	3
69	2.00	.	.	.	.	.	.
70	2.00	.	.	.	.	.	.
71	2.00	.	.	.	.	.	.
72	2.00	.	.	.	.	.	.
73	2.00	.	.	.	.	.	.
74	2.00	.	.	.	.	.	.
75	2.00	.	.	.	.	.	.
76	2.00	.	.	.	.	.	.
77	2.00	.	.	.	.	.	.
78	2.00	.	.	.	.	.	.
79	2.00	.	.	.	.	.	.
80	2.00	.	.	.	.	.	.
81	2.00	.	.	.	.	.	.
82	2.00	.	.	.	.	.	.
83	2.00	.	.	.	.	.	.
84	2.00	.	.	.	.	.	.
85	2.00	.	.	.	.	.	.
86	2.00	.	.	.	.	.	.
87	2.00	.	.	.	.	.	.
88	2.00	.	.	.	.	.	.
89	2.00	.	.	.	.	.	.
90	2.00	.	.	.	.	.	.
91	2.00	.	.	.	.	.	.
92	2.00	.	.	.	.	.	.
93	2.00	.	.	.	.	.	.
94	2.00	.	.	.	.	.	.
95	2.00	.	.	.	.	.	.
96	2.00	.	.	.	.	.	.
97	2.00	.	.	.	.	.	.
98	2.00	.	.	.	.	.	.
99	2.00	.	.	.	.	.	.
100	2.00	.	.	.	.	.	.

	قسم	العاملين	سياسة	حدوث	v11	v12	v13
51	2	.	2.00	5.00	5	4	4
52	2	.	2.00	5.00	4	4	2
53	2	.	2.00	5.00	4	4	2
54	2	.	2.00	5.00	5	4	2
55	2	.	2.00	5.00	4	4	5
56	1	1	1.00	5.00	5	4	2
57	1	3	1.00	4.00	5	3	4
58	1	2	1.00	4.00	5	4	4
59	1	3	1.00	3.00	5	3	4
60	1	3	1.00	5.00	5	5	5
61	1	5	1.00	5.00	5	5	5
62	1	5	1.00	1.00	5	3	2
63	1	2	1.00	4.00	5	4	4
64	1	3	1.00	5.00	5	3	4
65	1	3	1.00	2.00	5	4	5
66	1	2	1.00	5.00	5	3	5
67	1	3	1.00	5.00	5	4	4
68	1	2	1.00	2.00	5	4	4
69	.	.	.	.	4	3	4
70	.	.	.	.	2	4	2
71	.	.	.	.	3	5	4
72	.	.	.	.	3	3	2
73	.	.	.	.	4	5	2
74	.	.	.	.	4	3	4
75	.	.	.	.	4	3	2
76	.	.	.	.	5	3	4
77	.	.	.	.	3	3	2
78	.	.	.	.	3	3	2
79	.	.	.	.	4	3	4
80	.	.	.	.	4	5	2
81	.	.	.	.	3	2	4
82	.	.	.	.	3	5	2
83	.	.	.	.	5	5	2
84	.	.	.	.	4	3	4
85	.	.	.	.	4	5	2
86	.	.	.	.	5	5	4
87	.	.	.	.	5	5	2
88	.	.	.	.	1	3	2
89	.	.	.	.	4	3	4
90	.	.	.	.	5	5	2
91	.	.	.	.	4	3	4
92	.	.	.	.	4	5	2
93	.	.	.	.	5	5	4
94	.	.	.	.	5	5	2
95	.	.	.	.	4	5	2
96	.	.	.	.	4	3	4
97	.	.	.	.	5	4	2
98	.	.	.	.	4	3	4
99	.	.	.	.	2	5	2
100	.	.	.	.	3	5	4

	v14	v15	v16	v17	v18	v19	v20
51	6	4	3	4	4	2	4
52	6	5	3	3	4	2	4
53	6	4	3	4	4	2	3
54	6	4	3	4	1	2	4
55	3	5	3	4	4	3	4
56	4	4	3	4	4	1	4
57	5	5	4	2	1	2	4
58	4	5	3	1	5	3	3
59	4	5	4	2	4	1	2
60	5	5	2	1	1	3	4
61	4	5	2	1	4	2	4
62	5	5	4	2	1	2	2
63	4	5	3	1	5	3	3
64	4	4	4	3	5	2	2
65	5	5	4	3	1	2	2
66	5	5	4	2	1	2	4
67	5	5	4	3	4	2	4
68	4	5	3	1	5	3	3
69	2	5	4	4	4	3	3
70	2	3	4	2	2	3	3
71	3	5	3	3	2	2	2
72	2	3	4	2	2	3	3
73	2	3	4	2	2	3	3
74	2	5	4	4	4	3	3
75	2	3	4	2	2	3	3
76	3	5	3	3	2	2	2
77	2	3	4	2	2	3	3
78	4	3	4	2	2	3	3
79	2	5	4	4	4	3	3
80	2	3	4	2	2	3	3
81	4	5	3	3	2	2	2
82	2	3	4	2	2	3	3
83	2	3	5	2	2	2	3
84	4	5	4	4	4	3	3
85	5	3	4	3	2	3	3
86	4	5	3	3	2	2	2
87	2	3	4	2	2	3	3
88	2	3	4	2	2	3	3
89	2	5	4	4	4	3	3
90	2	3	4	2	2	2	3
91	4	5	5	3	4	3	3
92	4	3	4	2	2	3	3
93	4	5	3	3	2	2	2
94	2	3	4	2	2	3	3
95	3	3	4	2	2	2	3
96	5	5	4	4	4	3	3
97	4	3	4	2	2	2	3
98	2	5	4	4	4	3	3
99	4	3	4	2	2	3	3
100	3	5	3	3	2	2	2

	v21	التلاعب	البرامج	البيانات	تدمير	تعطيل	تنصت
51	4	4	5	4.00	3	3	3
52	4	5	4	4.00	1	1	1
53	4	5	4	4.00	3	1	3
54	4	5	4	4.00	4	3	3
55	4	4	5	4.00	3	2	3
56	4	5	4	4.00	3	3	3
57	3	1	5	1.00	4	2	1
58	4	4	4	4.00	4	5	4
59	3	2	4	2.00	4	4	1
60	3	4	4	1.00	2	4	1
61	4	2	2	4.00	2	4	1
62	3	4	4	4.00	2	3	2
63	4	4	4	4.00	4	4	4
64	3	4	4	1.00	2	4	1
65	3	2	4	4.00	2	4	1
66	3	4	5	3.00	2	4	2
67	3	4	4	2.00	3	2	1
68	4	4	4	4.00	4	5	4
69	2	3	3	3.00	3	1	4
70	2	5	4	3.00	5	4	3
71	2	4	5	4.00	3	4	3
72	2	3	3	3.00	3	4	4
73	2	3	3	3.00	3	3	4
74	3	3	3	3.00	3	3	4
75	2	5	4	3.00	4	3	3
76	3	3	2	2.00	3	4	3
77	2	3	3	3.00	2	2	4
78	2	5	3	3.00	3	3	4
79	3	3	3	3.00	3	3	4
80	2	5	4	3.00	4	3	3
81	3	4	5	4.00	3	4	3
82	2	3	3	3.00	3	4	4
83	3	3	3	3.00	3	2	4
84	2	3	3	3.00	3	4	4
85	3	5	4	3.00	4	2	3
86	2	4	5	4.00	3	1	3
87	2	3	3	3.00	3	4	4
88	3	3	3	3.00	3	4	4
89	2	3	4	3.00	3	1	4
90	2	5	3	3.00	4	4	4
91	2	3	3	3.00	3	4	4
92	4	5	4	3.00	4	4	4
93	2	4	5	4.00	3	3	3
94	3	3	3	3.00	3	4	4
95	2	3	3	3.00	3	4	4
96	2	3	3	2.00	2	4	4
97	2	3	3	3.00	3	2	4
98	3	3	3	3.00	3	1	4
99	2	5	4	3.00	4	1	3
100	3	4	3	4.00	3	1	3

	نسخ	برامجها	استيلاء	أحصنة	فيروسات	أختراقات	إعتراض
51	4	5	4	4	5	3	3
52	2	4	1	1	1	1	1
53	4	5	4	4	5	3	3
54	4	4	4	4	5	2	3
55	2	5	3	3	5	3	3
56	4	5	4	4	5	3	3
57	1	2	4	3	1	1	3
58	2	5	3	5	5	5	2
59	1	2	4	4	1	1	3
60	2	2	3	2	2	3	1
61	1	2	2	5	3	2	1
62	3	3	3	5	4	3	3
63	2	5	3	5	5	5	2
64	1	2	3	2	3	3	3
65	1	2	2	4	2	3	3
66	1	2	2	2	3	1	3
67	3	3	2	4	4	3	3
68	2	5	3	5	5	5	2
69	4	5	3	4	4	4	3
70	3	5	3	4	4	4	3
71	4	5	5	4	5	4	4
72	4	5	3	4	4	4	3
73	4	5	3	4	4	4	3
74	4	5	3	4	4	4	3
75	3	5	3	4	4	4	3
76	4	5	5	4	5	4	4
77	4	5	3	4	4	4	3
78	4	5	3	4	4	4	3
79	4	5	3	4	4	4	3
80	3	3	3	4	4	4	3
81	4	5	5	4	5	4	4
82	4	5	3	4	4	4	3
83	4	3	3	4	4	4	3
84	4	5	3	4	4	4	3
85	3	3	3	4	4	4	3
86	4	5	5	4	5	4	4
87	4	5	3	4	4	4	3
88	4	5	3	4	4	4	3
89	4	5	3	4	4	4	3
90	4	5	3	4	4	4	3
91	4	3	3	4	4	4	3
92	3	5	3	4	4	4	3
93	4	5	5	4	5	4	4
94	4	3	3	4	4	4	3
95	3	5	3	4	4	4	3
96	4	4	3	4	4	4	3
97	4	5	3	4	4	4	3
98	4	3	3	4	4	4	3
99	3	5	3	4	4	4	3
100	4	3	5	4	5	4	4

	إغراق	أفشاء	محاولة	فك	lan	الأقرص	wan
51	2	5.00	5.00	4.00	4.00	2.00	4.00
52	1	5.00	4.00	4.00	4.00	4.00	4.00
53	2	5.00	5.00	4.00	4.00	4.00	4.00
54	3	5.00	5.00	4.00	4.00	3.00	4.00
55	2	5.00	3.00	4.00	4.00	3.00	4.00
56	3	5.00	5.00	4.00	4.00	4.00	4.00
57	1	3.00	4.00	1.00	2.00	3.00	2.00
58	4	4.00	4.00	4.00	3.00	5.00	5.00
59	1	3.00	4.00	1.00	2.00	3.00	2.00
60	1	1.00	2.00	2.00	4.00	3.00	1.00
61	1	1.00	2.00	1.00	3.00	3.00	1.00
62	1	3.00	4.00	2.00	3.00	2.00	2.00
63	4	4.00	4.00	4.00	3.00	5.00	5.00
64	1	3.00	4.00	3.00	4.00	3.00	2.00
65	1	3.00	3.00	1.00	3.00	3.00	2.00
66	1	3.00	2.00	4.00	3.00	3.00	2.00
67	2	3.00	3.00	4.00	3.00	3.00	2.00
68	4	4.00	4.00	4.00	3.00	5.00	5.00
69	3	.	.	.	.	.	.
70	5	.	.	.	.	.	.
71	5	.	.	.	.	.	.
72	3	.	.	.	.	.	.
73	3	.	.	.	.	.	.
74	3	.	.	.	.	.	.
75	5	.	.	.	.	.	.
76	5	.	.	.	.	.	.
77	3	.	.	.	.	.	.
78	3	.	.	.	.	.	.
79	3	.	.	.	.	.	.
80	5	.	.	.	.	.	.
81	5	.	.	.	.	.	.
82	3	.	.	.	.	.	.
83	3	.	.	.	.	.	.
84	3	.	.	.	.	.	.
85	5	.	.	.	.	.	.
86	5	.	.	.	.	.	.
87	3	.	.	.	.	.	.
88	3	.	.	.	.	.	.
89	3	.	.	.	.	.	.
90	3	.	.	.	.	.	.
91	3	.	.	.	.	.	.
92	5	.	.	.	.	.	.
93	5	.	.	.	.	.	.
94	3	.	.	.	.	.	.
95	3	.	.	.	.	.	.
96	3	.	.	.	.	.	.
97	3	.	.	.	.	.	.
98	3	.	.	.	.	.	.
99	5	.	.	.	.	.	.
100	5	.	.	.	.	.	.

	internet	vpn	عسكرية	إبراز	تجارية	تسلية	انتقام
51	5.00	3.00	1.00	5.00	2.00	5.00	4.00
52	2.00	4.00	1.00	5.00	4.00	5.00	4.00
53	5.00	4.00	1.00	5.00	2.00	5.00	4.00
54	5.00	2.00	1.00	5.00	3.00	5.00	4.00
55	5.00	2.00	1.00	5.00	4.00	5.00	4.00
56	5.00	4.00	1.00	5.00	1.00	5.00	3.00
57	2.00	1.00	1.00	2.00	4.00	3.00	3.00
58	5.00	1.00	1.00	4.00	1.00	5.00	4.00
59	2.00	1.00	1.00	2.00	4.00	3.00	1.00
60	2.00	1.00	1.00	3.00	4.00	1.00	2.00
61	2.00	1.00	1.00	5.00	3.00	4.00	1.00
62	2.00	1.00	1.00	2.00	2.00	4.00	1.00
63	5.00	1.00	1.00	4.00	1.00	5.00	4.00
64	4.00	1.00	2.00	2.00	3.00	4.00	1.00
65	2.00	1.00	1.00	2.00	1.00	4.00	1.00
66	2.00	1.00	1.00	5.00	3.00	3.00	4.00
67	5.00	1.00	1.00	4.00	4.00	5.00	1.00
68	5.00	1.00	1.00	4.00	1.00	5.00	4.00
69	.	.	4.00	5.00	4.00	5.00	5.00
70	.	.	3.00	5.00	4.00	4.00	4.00
71	.	.	4.00	5.00	4.00	4.00	3.00
72	.	.	4.00	4.00	4.00	5.00	5.00
73	.	.	4.00	4.00	4.00	5.00	5.00
74	.	.	4.00	4.00	4.00	3.00	5.00
75	.	.	3.00	4.00	4.00	4.00	4.00
76	.	.	4.00	4.00	4.00	4.00	3.00
77	.	.	4.00	4.00	4.00	5.00	5.00
78	.	.	4.00	4.00	4.00	3.00	3.00
79	.	.	4.00	4.00	4.00	5.00	5.00
80	.	.	3.00	2.00	4.00	3.00	4.00
81	.	.	4.00	4.00	3.00	4.00	3.00
82	.	.	4.00	4.00	3.00	3.00	5.00
83	.	.	4.00	4.00	3.00	3.00	5.00
84	.	.	4.00	4.00	3.00	3.00	5.00
85	.	.	3.00	4.00	3.00	4.00	4.00
86	.	.	4.00	4.00	3.00	4.00	3.00
87	.	.	4.00	4.00	4.00	5.00	5.00
88	.	.	4.00	3.00	4.00	5.00	5.00
89	.	.	4.00	3.00	4.00	5.00	5.00
90	.	.	4.00	5.00	3.00	5.00	5.00
91	.	.	4.00	3.00	3.00	5.00	5.00
92	.	.	3.00	3.00	3.00	4.00	4.00
93	.	.	4.00	3.00	3.00	4.00	3.00
94	.	.	4.00	3.00	4.00	5.00	5.00
95	.	.	4.00	3.00	4.00	5.00	4.00
96	.	.	4.00	4.00	4.00	5.00	5.00
97	.	.	4.00	3.00	4.00	5.00	5.00
98	.	.	4.00	3.00	4.00	5.00	5.00
99	.	.	3.00	4.00	4.00	4.00	4.00
100	.	.	4.00	3.00	4.00	4.00	3.00

	الشخصية	التكلفة	الإنذرات	الضعف	فيروس	طروادة	spoofing
51	5.00	2.00	.	4.000	5.00	5.00	4.00
52	5.00	2.00	.	4.000	5.00	5.00	4.00
53	4.00	2.00	.	4.000	5.00	5.00	4.00
54	5.00	2.00	.	4.000	5.00	5.00	4.00
55	5.00	2.00	.	4.000	5.00	4.00	4.00
56	5.00	2.00	.	4.000	5.00	5.00	4.00
57	3.00	1.00	1.00	2.000	2.00	5.00	2.00
58	2.00	1.00	4.00	4.000	5.00	5.00	5.00
59	3.00	1.00	2.00	2.000	5.00	5.00	5.00
60	3.00	1.00	.	1.000	5.00	5.00	3.00
61	3.00	1.00	.	1.000	5.00	5.00	2.00
62	4.00	1.00	1.00	2.000	5.00	5.00	2.00
63	2.00	1.00	1.00	4.000	5.00	5.00	5.00
64	4.00	1.00	2.00	2.000	5.00	5.00	4.00
65	3.00	1.00	1.00	2.000	5.00	3.00	2.00
66	3.00	1.00	1.00	2.000	4.00	5.00	2.00
67	3.00	1.00	1.00	2.000	5.00	5.00	2.00
68	2.00	1.00	3.00	4.000	5.00	5.00	5.00
69	5.00	.	.	.	.	.	.
70	5.00	.	.	.	.	.	.
71	4.00	.	.	.	.	.	.
72	5.00	.	.	.	.	.	.
73	5.00	.	.	.	.	.	.
74	5.00	.	.	.	.	.	.
75	5.00	.	.	.	.	.	.
76	4.00	.	.	.	.	.	.
77	5.00	.	.	.	.	.	.
78	3.00	.	.	.	.	.	.
79	5.00	.	.	.	.	.	.
80	3.00	.	.	.	.	.	.
81	3.00	.	.	.	.	.	.
82	3.00	.	.	.	.	.	.
83	3.00	.	.	.	.	.	.
84	5.00	.	.	.	.	.	.
85	3.00	.	.	.	.	.	.
86	4.00	.	.	.	.	.	.
87	3.00	.	.	.	.	.	.
88	4.00	.	.	.	.	.	.
89	5.00	.	.	.	.	.	.
90	5.00	.	.	.	.	.	.
91	5.00	.	.	.	.	.	.
92	5.00	.	.	.	.	.	.
93	4.00	.	.	.	.	.	.
94	5.00	.	.	.	.	.	.
95	3.00	.	.	.	.	.	.
96	3.00	.	.	.	.	.	.
97	3.00	.	.	.	.	.	.
98	5.00	.	.	.	.	.	.
99	5.00	.	.	.	.	.	.
100	4.00	.	.	.	.	.	.

	انتحال	المنافذ	التشارك	الثغرات	ثغراتتح	برمجة	إرفاق
51	4.00	4.00	5.00	5.00	4.00	4.00	3.00
52	4.00	4.00	5.00	5.00	4.00	4.00	3.00
53	4.00	4.00	5.00	5.00	4.00	4.00	3.00
54	4.00	4.00	5.00	5.00	4.00	4.00	3.00
55	4.00	4.00	5.00	5.00	4.00	4.00	3.00
56	4.00	4.00	5.00	5.00	4.00	4.00	3.00
57	1.00	2.00	1.00	1.00	2.00	1.00	1.00
58	2.00	4.00	5.00	4.00	2.00	4.00	4.00
59	2.00	4.00	5.00	4.00	2.00	4.00	4.00
60	1.00	2.00	1.00	2.00	1.00	1.00	2.00
61	1.00	2.00	4.00	2.00	1.00	1.00	2.00
62	2.00	2.00	1.00	2.00	2.00	1.00	1.00
63	2.00	4.00	5.00	4.00	2.00	4.00	4.00
64	1.00	2.00	4.00	2.00	2.00	1.00	1.00
65	2.00	4.00	1.00	2.00	2.00	1.00	1.00
66	1.00	2.00	4.00	2.00	2.00	1.00	1.00
67	1.00	2.00	1.00	1.00	2.00	1.00	1.00
68	2.00	4.00	5.00	4.00	2.00	4.00	4.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	التخفي	المزودات	السرقة	تشغيل	ترك	زراعة	القانوني
51	4.00	5.00	5.00	3.00	4.00	2.00	4.00
52	4.00	5.00	5.00	3.00	4.00	2.00	4.00
53	4.00	5.00	5.00	3.00	3.00	2.00	4.00
54	4.00	5.00	5.00	3.00	4.00	2.00	4.00
55	4.00	5.00	5.00	3.00	4.00	2.00	4.00
56	4.00	5.00	5.00	3.00	4.00	2.00	4.00
57	2.00	1.00	1.00	1.00	3.00	1.00	1.00
58	3.00	3.00	1.00	3.00	2.00	2.00	3.00
59	3.00	3.00	1.00	3.00	2.00	2.00	3.00
60	1.00	1.00	1.00	1.00	1.00	1.00	1.00
61	1.00	1.00	1.00	1.00	1.00	1.00	1.00
62	2.00	1.00	1.00	1.00	3.00	1.00	1.00
63	3.00	3.00	1.00	3.00	2.00	2.00	3.00
64	2.00	1.00	1.00	1.00	3.00	2.00	2.00
65	2.00	1.00	1.00	1.00	3.00	2.00	1.00
66	2.00	1.00	1.00	1.00	3.00	2.00	2.00
67	2.00	1.00	1.00	1.00	3.00	1.00	2.00
68	3.00	3.00	1.00	3.00	2.00	2.00	3.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	الصيانة	مرخص	غمرخص	مجاني	غمجاني	cookies	groove
51	3.00	3.00	5.00	5.00	4.00	5.00	3.00
52	3.00	3.00	5.00	5.00	4.00	5.00	1.00
53	3.00	2.00	5.00	5.00	4.00	5.00	1.00
54	3.00	3.00	5.00	5.00	4.00	5.00	3.00
55	3.00	3.00	5.00	5.00	4.00	5.00	2.00
56	3.00	3.00	5.00	4.00	4.00	5.00	1.00
57	1.00	1.00	4.00	5.00	3.00	4.00	2.00
58	2.00	3.00	5.00	5.00	3.00	3.00	2.00
59	2.00	3.00	5.00	5.00	3.00	4.00	2.00
60	1.00	3.00	5.00	4.00	4.00	3.00	2.00
61	1.00	3.00	5.00	5.00	4.00	3.00	3.00
62	1.00	1.00	4.00	5.00	3.00	4.00	2.00
63	2.00	3.00	5.00	5.00	3.00	3.00	2.00
64	1.00	3.00	4.00	5.00	3.00	4.00	2.00
65	1.00	1.00	4.00	5.00	3.00	4.00	2.00
66	2.00	3.00	4.00	5.00	3.00	4.00	2.00
67	2.00	2.00	4.00	5.00	3.00	4.00	2.00
68	2.00	3.00	5.00	5.00	3.00	3.00	2.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	caligula	netbus	subseven	hack	wincrash	tfn	toolkit
51	3.00	2.00	4.00	3.00	4.00	3.00	4.00
52	2.00	4.00	5.00	3.00	4.00	3.00	4.00
53	3.00	4.00	4.00	3.00	4.00	3.00	4.00
54	3.00	4.00	4.00	4.00	4.00	3.00	3.00
55	2.00	4.00	4.00	4.00	4.00	3.00	4.00
56	3.00	4.00	4.00	3.00	4.00	3.00	4.00
57	2.00	2.00	2.00	2.00	2.00	2.00	2.00
58	2.00	3.00	3.00	3.00	3.00	5.00	5.00
59	2.00	3.00	5.00	2.00	2.00	2.00	2.00
60	2.00	3.00	3.00	3.00	4.00	5.00	5.00
61	2.00	2.00	4.00	2.00	2.00	3.00	2.00
62	2.00	3.00	2.00	2.00	2.00	2.00	2.00
63	2.00	3.00	3.00	3.00	3.00	5.00	5.00
64	2.00	2.00	2.00	2.00	2.00	2.00	2.00
65	2.00	2.00	5.00	2.00	4.00	4.00	2.00
66	2.00	4.00	2.00	2.00	3.00	2.00	2.00
67	2.00	2.00	2.00	2.00	2.00	2.00	2.00
68	2.00	3.00	3.00	3.00	3.00	5.00	5.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	msword	msexcel	revelat	icq	بتنصت	بالتغيل	المشاركة
51	3.00	3.00	3.00	3.00	5.00	3.00	5.00
52	3.00	3.00	3.00	3.00	5.00	2.00	5.00
53	3.00	3.00	3.00	3.00	5.00	3.00	5.00
54	3.00	3.00	2.00	3.00	5.00	2.00	5.00
55	4.00	4.00	3.00	3.00	5.00	3.00	5.00
56	3.00	3.00	3.00	3.00	5.00	3.00	5.00
57	2.00	2.00	2.00	2.00	5.00	3.00	3.00
58	4.00	4.00	2.00	5.00	5.00	3.00	5.00
59	2.00	2.00	2.00	2.00	3.00	3.00	3.00
60	4.00	4.00	2.00	5.00	5.00	3.00	5.00
61	2.00	2.00	2.00	3.00	2.00	2.00	2.00
62	2.00	2.00	1.00	2.00	3.00	4.00	3.00
63	4.00	4.00	2.00	5.00	5.00	3.00	5.00
64	2.00	2.00	2.00	3.00	3.00	2.00	3.00
65	2.00	2.00	3.00	2.00	3.00	2.00	3.00
66	3.00	3.00	2.00	3.00	3.00	4.00	3.00
67	2.00	2.00	3.00	4.00	3.00	2.00	3.00
68	4.00	4.00	2.00	5.00	5.00	3.00	5.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	البريد	الديدان	التقنية	الحمايةت	تكلفةلتو	تكلفةستخ	مصدر
51	5.00	5.00	4.00	5.00	5.00	5.00	4.00
52	5.00	5.00	4.00	5.00	5.00	5.00	4.00
53	5.00	5.00	4.00	5.00	5.00	5.00	4.00
54	5.00	5.00	4.00	5.00	5.00	5.00	4.00
55	5.00	5.00	4.00	5.00	5.00	5.00	4.00
56	5.00	5.00	4.00	5.00	5.00	5.00	4.00
57	3.00	3.00	4.00	4.00	4.00	3.00	4.00
58	5.00	5.00	5.00	5.00	4.00	4.00	4.00
59	3.00	3.00	5.00	5.00	4.00	4.00	4.00
60	5.00	5.00	4.00	3.00	4.00	3.00	4.00
61	3.00	3.00	4.00	3.00	4.00	3.00	4.00
62	4.00	4.00	5.00	5.00	4.00	4.00	4.00
63	5.00	5.00	5.00	5.00	4.00	4.00	4.00
64	4.00	4.00	5.00	5.00	4.00	4.00	5.00
65	4.00	4.00	5.00	5.00	4.00	4.00	4.00
66	4.00	4.00	5.00	5.00	4.00	4.00	4.00
67	4.00	5.00	5.00	5.00	4.00	4.00	4.00
68	5.00	5.00	5.00	5.00	4.00	4.00	4.00
69	.	.	4.00	5.00	3.00	3.00	5.00
70	.	.	3.00	3.00	4.00	4.00	2.00
71	.	.	4.00	4.00	2.00	2.00	4.00
72	.	.	4.00	5.00	3.00	3.00	5.00
73	.	.	4.00	5.00	3.00	3.00	5.00
74	.	.	4.00	5.00	3.00	3.00	5.00
75	.	.	3.00	3.00	4.00	4.00	2.00
76	.	.	3.00	4.00	2.00	2.00	4.00
77	.	.	4.00	5.00	4.00	3.00	5.00
78	.	.	3.00	5.00	3.00	3.00	5.00
79	.	.	4.00	5.00	3.00	4.00	5.00
80	.	.	3.00	3.00	4.00	4.00	2.00
81	.	.	4.00	4.00	2.00	2.00	4.00
82	.	.	4.00	5.00	3.00	3.00	5.00
83	.	.	4.00	5.00	3.00	3.00	5.00
84	.	.	4.00	5.00	4.00	3.00	5.00
85	.	.	3.00	3.00	4.00	4.00	2.00
86	.	.	4.00	4.00	2.00	2.00	4.00
87	.	.	4.00	5.00	3.00	3.00	5.00
88	.	.	2.00	3.00	2.00	3.00	5.00
89	.	.	4.00	5.00	3.00	3.00	4.00
90	.	.	4.00	5.00	3.00	3.00	5.00
91	.	.	4.00	5.00	3.00	3.00	2.00
92	.	.	2.00	3.00	4.00	4.00	2.00
93	.	.	4.00	4.00	2.00	2.00	4.00
94	.	.	2.00	5.00	3.00	3.00	5.00
95	.	.	3.00	5.00	3.00	3.00	5.00
96	.	.	4.00	5.00	3.00	3.00	5.00
97	.	.	4.00	5.00	3.00	3.00	5.00
98	.	.	4.00	5.00	3.00	3.00	5.00
99	.	.	3.00	3.00	4.00	4.00	2.00
100	.	.	5.00	4.00	2.00	2.00	4.00

	var00001	ip	حمايةتتع	ضبط	دليل	الديي	الد
51	4.00	7.00	7.00	3.00	.	.	.
52	2.00	7.00	6.00	3.00	.	.	.
53	2.00	7.00	6.00	3.00	.	.	.
54	2.00	6.00	6.00	3.00	.	.	.
55	2.00	5.00	6.00	1.00	.	.	.
56	3.00	5.00	6.00	3.00	.	.	.
57	2.00	7.00	6.00	3.00	.	.	.
58	2.00	7.00	7.00	1.00	.	.	.
59	2.00	7.00	6.00	1.00	.	.	.
60	4.00	6.00	6.00	3.00	.	.	.
61	3.00	7.00	6.00	3.00	.	.	.
62	2.00	7.00	7.00	1.00	.	.	.
63	2.00	7.00	7.00	3.00	.	.	.
64	2.00	7.00	6.00	3.00	.	.	.
65	4.00	7.00	7.00	1.00	.	.	.
66	4.00	7.00	6.00	3.00	.	.	.
67	2.00	7.00	6.00	3.00	.	.	.
68	3.00	7.00	7.00	3.00	.	.	.
69	5.00	7.00	6.00	3.00	5.00	4.00	4.00
70	2.00	5.00	6.00	3.00	5.00	3.00	3.00
71	4.00	5.00	6.00	3.00	5.00	4.00	4.00
72	3.00	7.00	6.00	3.00	5.00	4.00	4.00
73	3.00	7.00	6.00	3.00	5.00	4.00	4.00
74	5.00	8.00	6.00	3.00	5.00	4.00	4.00
75	2.00	7.00	6.00	2.00	5.00	4.00	4.00
76	3.00	7.00	6.00	3.00	5.00	4.00	4.00
77	5.00	7.00	6.00	3.00	5.00	4.00	4.00
78	4.00	7.00	6.00	3.00	3.00	2.00	4.00
79	4.00	7.00	6.00	3.00	5.00	4.00	2.00
80	2.00	7.00	4.00	1.00	5.00	4.00	4.00
81	4.00	2.00	3.00	3.00	5.00	4.00	4.00
82	4.00	3.00	2.00	1.00	4.00	4.00	3.00
83	5.00	7.00	3.00	3.00	4.00	4.00	3.00
84	5.00	1.00	6.00	2.00	4.00	4.00	3.00
85	2.00	7.00	6.00	2.00	4.00	4.00	3.00
86	4.00	6.00	6.00	1.00	1.00	5.00	1.00
87	5.00	8.00	3.00	2.00	4.00	4.00	4.00
88	5.00	7.00	1.00	1.00	4.00	4.00	3.00
89	2.00	8.00	6.00	2.00	4.00	4.00	4.00
90	5.00	7.00	2.00	3.00	4.00	4.00	5.00
91	2.00	7.00	6.00	3.00	5.00	4.00	4.00
92	2.00	2.00	6.00	3.00	5.00	4.00	4.00
93	3.00	7.00	6.00	2.00	5.00	4.00	4.00
94	3.00	2.00	6.00	2.00	5.00	4.00	4.00
95	5.00	3.00	6.00	2.00	5.00	4.00	4.00
96	2.00	7.00	6.00	2.00	5.00	4.00	4.00
97	5.00	1.00	6.00	2.00	5.00	3.00	2.00
98	5.00	7.00	6.00	2.00	5.00	4.00	4.00
99	2.00	6.00	6.00	3.00	5.00	4.00	4.00
100	4.00	8.00	6.00	3.00	3.00	4.00	3.00

	var00005	البلاغ	كفاءة	الخوف	الرغبة	اكتشاف	محدودية
51	.	5.00	2.00	4.00	4.00	4.00	4.00
52	.	5.00	2.00	4.00	4.00	3.00	4.00
53	.	5.00	2.00	4.00	4.00	3.00	4.00
54	.	5.00	2.00	3.00	3.00	3.00	3.00
55	.	5.00	2.00	4.00	4.00	3.00	4.00
56	.	5.00	2.00	4.00	4.00	3.00	4.00
57	.	4.00	1.00	5.00	5.00	2.00	5.00
58	.	5.00	3.00	3.00	5.00	5.00	5.00
59	.	5.00	3.00	4.00	4.00	2.00	4.00
60	.	5.00	2.00	5.00	5.00	2.00	1.00
61	.	5.00	2.00	4.00	4.00	2.00	4.00
62	.	5.00	2.00	4.00	4.00	2.00	4.00
63	.	5.00	3.00	3.00	5.00	5.00	5.00
64	.	5.00	2.00	4.00	4.00	2.00	4.00
65	.	5.00	2.00	4.00	4.00	2.00	4.00
66	.	5.00	2.00	4.00	4.00	2.00	4.00
67	.	5.00	2.00	4.00	4.00	4.00	4.00
68	.	5.00	3.00	3.00	5.00	5.00	5.00
69	4.00	4.00	1.00	5.00	5.00	5.00	5.00
70	2.00	5.00	3.00	4.00	4.00	2.00	3.00
71	4.00	5.00	2.00	3.00	5.00	4.00	4.00
72	4.00	4.00	1.00	5.00	5.00	5.00	5.00
73	4.00	4.00	1.00	5.00	5.00	5.00	5.00
74	4.00	4.00	1.00	5.00	5.00	5.00	5.00
75	4.00	5.00	3.00	4.00	4.00	2.00	3.00
76	5.00	5.00	2.00	3.00	5.00	4.00	4.00
77	4.00	4.00	1.00	5.00	5.00	5.00	5.00
78	4.00	4.00	1.00	5.00	5.00	5.00	5.00
79	2.00	4.00	1.00	5.00	5.00	5.00	5.00
80	4.00	5.00	3.00	4.00	4.00	2.00	3.00
81	4.00	5.00	2.00	3.00	5.00	4.00	4.00
82	4.00	4.00	1.00	5.00	5.00	5.00	5.00
83	2.00	4.00	1.00	5.00	5.00	5.00	5.00
84	4.00	4.00	1.00	5.00	5.00	5.00	5.00
85	4.00	5.00	3.00	4.00	4.00	2.00	3.00
86	1.00	5.00	2.00	3.00	5.00	4.00	4.00
87	4.00	4.00	1.00	5.00	5.00	5.00	5.00
88	3.00	4.00	1.00	5.00	5.00	5.00	5.00
89	3.00	4.00	1.00	5.00	5.00	5.00	5.00
90	3.00	4.00	1.00	5.00	5.00	5.00	5.00
91	4.00	4.00	1.00	5.00	5.00	5.00	5.00
92	1.00	5.00	3.00	4.00	4.00	2.00	3.00
93	4.00	5.00	2.00	3.00	5.00	4.00	4.00
94	2.00	4.00	1.00	5.00	5.00	5.00	5.00
95	4.00	4.00	1.00	5.00	5.00	5.00	5.00
96	4.00	4.00	1.00	5.00	5.00	5.00	5.00
97	4.00	4.00	1.00	5.00	5.00	5.00	5.00
98	4.00	4.00	1.00	5.00	5.00	5.00	5.00
99	4.00	5.00	3.00	4.00	4.00	2.00	3.00
100	4.00	5.00	2.00	3.00	5.00	4.00	4.00

	التشفير	سجل	auditing	مراقبة	الشبكة	report	مراجعة
51	3.00	5.00	5.00	5.00	4.00	5.00	4.00
52	4.00	5.00	5.00	5.00	4.00	5.00	4.00
53	4.00	5.00	5.00	5.00	4.00	5.00	4.00
54	4.00	5.00	5.00	5.00	4.00	5.00	4.00
55	4.00	5.00	5.00	5.00	4.00	5.00	4.00
56	4.00	5.00	5.00	5.00	4.00	5.00	4.00
57	5.00	5.00	5.00	5.00	4.00	4.00	4.00
58	2.00	5.00	5.00	4.00	3.00	4.00	3.00
59	5.00	5.00	5.00	5.00	4.00	5.00	5.00
60	2.00	5.00	4.00	4.00	3.00	5.00	4.00
61	2.00	5.00	4.00	4.00	3.00	5.00	4.00
62	3.00	5.00	5.00	5.00	4.00	5.00	5.00
63	2.00	5.00	5.00	4.00	3.00	4.00	3.00
64	3.00	5.00	5.00	5.00	4.00	5.00	5.00
65	3.00	5.00	5.00	5.00	4.00	5.00	5.00
66	3.00	5.00	5.00	5.00	4.00	5.00	5.00
67	3.00	5.00	5.00	5.00	4.00	5.00	5.00
68	2.00	5.00	5.00	4.00	3.00	4.00	3.00
69	5.00	5.00	5.00	5.00	5.00	5.00	5.00
70	4.00	4.00	4.00	3.00	3.00	4.00	4.00
71	5.00	5.00	5.00	5.00	3.00	5.00	4.00
72	5.00	5.00	5.00	5.00	5.00	5.00	5.00
73	5.00	5.00	5.00	5.00	5.00	5.00	5.00
74	5.00	5.00	5.00	5.00	5.00	5.00	5.00
75	4.00	4.00	4.00	3.00	3.00	4.00	4.00
76	5.00	5.00	5.00	5.00	3.00	5.00	4.00
77	5.00	5.00	5.00	5.00	5.00	5.00	5.00
78	5.00	5.00	5.00	5.00	5.00	5.00	5.00
79	5.00	5.00	5.00	5.00	5.00	5.00	5.00
80	4.00	4.00	4.00	3.00	3.00	4.00	4.00
81	5.00	5.00	5.00	5.00	3.00	5.00	4.00
82	5.00	5.00	5.00	5.00	5.00	5.00	5.00
83	5.00	5.00	5.00	5.00	5.00	5.00	5.00
84	5.00	5.00	5.00	5.00	5.00	5.00	5.00
85	4.00	4.00	4.00	3.00	3.00	4.00	4.00
86	5.00	5.00	5.00	5.00	3.00	5.00	4.00
87	5.00	5.00	5.00	5.00	5.00	5.00	5.00
88	5.00	5.00	5.00	5.00	5.00	5.00	5.00
89	5.00	5.00	5.00	5.00	5.00	5.00	5.00
90	5.00	5.00	5.00	5.00	5.00	5.00	5.00
91	5.00	5.00	5.00	5.00	5.00	5.00	5.00
92	4.00	4.00	4.00	3.00	3.00	4.00	4.00
93	5.00	5.00	5.00	5.00	3.00	5.00	4.00
94	5.00	5.00	5.00	5.00	5.00	5.00	5.00
95	5.00	5.00	5.00	5.00	5.00	5.00	5.00
96	5.00	5.00	5.00	5.00	5.00	5.00	5.00
97	5.00	5.00	5.00	5.00	5.00	5.00	5.00
98	5.00	5.00	5.00	5.00	5.00	5.00	5.00
99	4.00	4.00	4.00	3.00	3.00	4.00	4.00
100	5.00	5.00	5.00	5.00	3.00	5.00	4.00

	الجدران	تتبعمختر	تتبعمصدر	كسر	كشف	viewdisk	pkzip
51	5.00	3.00	2.00	3.00	4.00	5.00	4.00
52	5.00	3.00	3.00	3.00	4.00	5.00	4.00
53	5.00	3.00	3.00	3.00	4.00	5.00	3.00
54	5.00	3.00	2.00	3.00	4.00	5.00	4.00
55	5.00	3.00	3.00	3.00	4.00	5.00	4.00
56	5.00	3.00	3.00	3.00	4.00	5.00	3.00
57	4.00	4.00	4.00	3.00	4.00	3.00	3.00
58	3.00	4.00	2.00	1.00	5.00	2.00	4.00
59	5.00	2.00	4.00	5.00	5.00	3.00	3.00
60	4.00	4.00	4.00	3.00	5.00	3.00	2.00
61	4.00	4.00	4.00	3.00	5.00	3.00	2.00
62	5.00	4.00	4.00	5.00	4.00	3.00	3.00
63	3.00	4.00	2.00	1.00	5.00	2.00	4.00
64	5.00	4.00	4.00	5.00	5.00	3.00	2.00
65	5.00	2.00	4.00	5.00	5.00	3.00	3.00
66	5.00	4.00	4.00	5.00	5.00	3.00	2.00
67	5.00	4.00	4.00	5.00	5.00	3.00	3.00
68	3.00	4.00	2.00	1.00	5.00	2.00	4.00
69	5.00	5.00	5.00	4.00	5.00	5.00	3.00
70	4.00	3.00	4.00	4.00	4.00	4.00	4.00
71	4.00	5.00	5.00	4.00	5.00	5.00	3.00
72	5.00	5.00	5.00	4.00	5.00	5.00	3.00
73	5.00	5.00	5.00	4.00	5.00	5.00	3.00
74	5.00	5.00	5.00	4.00	5.00	5.00	3.00
75	4.00	3.00	4.00	4.00	4.00	4.00	4.00
76	4.00	5.00	5.00	4.00	5.00	5.00	3.00
77	5.00	5.00	5.00	4.00	5.00	5.00	3.00
78	5.00	5.00	5.00	4.00	5.00	5.00	3.00
79	5.00	5.00	5.00	4.00	5.00	5.00	3.00
80	4.00	3.00	4.00	4.00	4.00	4.00	4.00
81	4.00	5.00	5.00	4.00	5.00	5.00	3.00
82	5.00	5.00	5.00	4.00	5.00	5.00	3.00
83	5.00	5.00	5.00	4.00	5.00	5.00	3.00
84	5.00	5.00	5.00	4.00	5.00	5.00	3.00
85	4.00	3.00	4.00	4.00	4.00	4.00	4.00
86	4.00	5.00	5.00	4.00	5.00	5.00	3.00
87	5.00	5.00	5.00	4.00	5.00	5.00	3.00
88	5.00	5.00	5.00	4.00	5.00	5.00	3.00
89	5.00	5.00	5.00	4.00	5.00	5.00	3.00
90	5.00	5.00	5.00	4.00	5.00	5.00	3.00
91	5.00	5.00	5.00	4.00	5.00	5.00	3.00
92	4.00	3.00	4.00	4.00	4.00	4.00	4.00
93	4.00	5.00	5.00	4.00	5.00	5.00	3.00
94	5.00	5.00	5.00	4.00	5.00	5.00	3.00
95	5.00	5.00	5.00	4.00	5.00	5.00	3.00
96	5.00	5.00	5.00	4.00	5.00	5.00	3.00
97	5.00	5.00	5.00	4.00	5.00	5.00	3.00
98	5.00	5.00	5.00	4.00	5.00	5.00	3.00
99	4.00	3.00	4.00	4.00	4.00	4.00	4.00
100	4.00	5.00	5.00	4.00	5.00	5.00	3.00

	xtreepro	lantast	diskette	laplink	المقارنة	logging	تشريعات
51	3.00	1.00	4.00	3.00	4.00	5.00	5.00
52	3.00	1.00	4.00	3.00	4.00	5.00	5.00
53	2.00	1.00	4.00	3.00	4.00	5.00	5.00
54	2.00	1.00	4.00	3.00	4.00	5.00	5.00
55	2.00	1.00	4.00	3.00	4.00	5.00	5.00
56	2.00	1.00	4.00	3.00	3.00	5.00	5.00
57	2.00	2.00	4.00	2.00	3.00	5.00	4.00
58	3.00	.	2.00	2.00	3.00	5.00	5.00
59	2.00	2.00	3.00	2.00	3.00	5.00	4.00
60	4.00	3.00	3.00	3.00	3.00	4.00	3.00
61	3.00	3.00	3.00	3.00	3.00	4.00	3.00
62	3.00	2.00	3.00	3.00	4.00	5.00	4.00
63	3.00	.	2.00	2.00	3.00	5.00	5.00
64	1.00	1.00	2.00	2.00	3.00	5.00	4.00
65	1.00	1.00	3.00	4.00	3.00	5.00	4.00
66	1.00	2.00	3.00	4.00	4.00	5.00	4.00
67	2.00	2.00	3.00	3.00	3.00	5.00	4.00
68	3.00	.	2.00	2.00	3.00	5.00	5.00
69	4.00	4.00	3.00	3.00	5.00	5.00	5.00
70	4.00	4.00	3.00	3.00	5.00	4.00	4.00
71	4.00	3.00	4.00	3.00	3.00	5.00	5.00
72	4.00	4.00	3.00	3.00	5.00	5.00	5.00
73	4.00	4.00	3.00	3.00	5.00	5.00	5.00
74	4.00	4.00	3.00	3.00	5.00	5.00	5.00
75	4.00	4.00	3.00	3.00	5.00	4.00	4.00
76	4.00	3.00	4.00	3.00	3.00	5.00	5.00
77	4.00	4.00	3.00	3.00	5.00	5.00	5.00
78	4.00	4.00	3.00	3.00	5.00	5.00	5.00
79	4.00	4.00	3.00	3.00	5.00	5.00	5.00
80	4.00	4.00	3.00	3.00	5.00	4.00	4.00
81	4.00	3.00	4.00	3.00	3.00	5.00	5.00
82	4.00	4.00	3.00	3.00	5.00	5.00	5.00
83	4.00	4.00	3.00	3.00	5.00	5.00	5.00
84	4.00	4.00	3.00	3.00	5.00	5.00	5.00
85	4.00	4.00	3.00	3.00	5.00	4.00	4.00
86	4.00	3.00	4.00	3.00	3.00	5.00	5.00
87	4.00	4.00	3.00	3.00	5.00	5.00	5.00
88	4.00	4.00	3.00	3.00	5.00	5.00	5.00
89	4.00	4.00	3.00	3.00	5.00	5.00	5.00
90	4.00	4.00	3.00	3.00	5.00	5.00	5.00
91	4.00	4.00	3.00	3.00	5.00	5.00	5.00
92	4.00	4.00	3.00	3.00	5.00	4.00	4.00
93	4.00	3.00	4.00	3.00	3.00	5.00	5.00
94	4.00	4.00	3.00	3.00	5.00	5.00	5.00
95	4.00	4.00	3.00	3.00	5.00	5.00	5.00
96	4.00	4.00	3.00	3.00	5.00	5.00	5.00
97	4.00	4.00	3.00	3.00	5.00	5.00	5.00
98	4.00	4.00	3.00	3.00	5.00	5.00	5.00
99	4.00	4.00	3.00	3.00	5.00	4.00	4.00
100	4.00	3.00	4.00	3.00	3.00	5.00	5.00

	مكونات	متخصص	التحقيق	مستجدات	تحديث	قناعة	الشكوى
51	4.00	3.00	5.00	3.00	2.00	1.00	5.00
52	4.00	3.00	5.00	3.00	2.00	1.00	5.00
53	4.00	3.00	5.00	3.00	2.00	1.00	5.00
54	4.00	3.00	5.00	3.00	2.00	1.00	5.00
55	4.00	3.00	5.00	3.00	2.00	1.00	5.00
56	4.00	3.00	5.00	3.00	2.00	1.00	5.00
57	3.00	2.00	5.00	3.00	4.00	3.00	4.00
58	4.00	3.00	3.00	3.00	3.00	2.00	5.00
59	3.00	2.00	5.00	3.00	4.00	3.00	4.00
60	3.00	2.00	2.00	2.00	2.00	4.00	3.00
61	3.00	2.00	2.00	2.00	2.00	4.00	3.00
62	3.00	2.00	5.00	3.00	4.00	3.00	4.00
63	4.00	3.00	3.00	3.00	3.00	2.00	5.00
64	3.00	2.00	5.00	3.00	4.00	3.00	4.00
65	3.00	2.00	5.00	3.00	4.00	3.00	4.00
66	3.00	2.00	5.00	3.00	4.00	3.00	4.00
67	3.00	2.00	5.00	3.00	4.00	3.00	4.00
68	4.00	3.00	3.00	3.00	3.00	2.00	5.00
69	3.00	5.00	2.00	3.00	4.00	4.00	3.00
70	3.00	3.00	2.00	3.00	2.00	4.00	5.00
71	5.00	4.00	2.00	5.00	4.00	2.00	4.00
72	3.00	5.00	2.00	2.00	2.00	5.00	5.00
73	3.00	5.00	2.00	2.00	2.00	5.00	5.00
74	3.00	5.00	2.00	3.00	4.00	4.00	3.00
75	3.00	3.00	2.00	3.00	2.00	4.00	5.00
76	5.00	4.00	2.00	5.00	4.00	2.00	4.00
77	3.00	5.00	2.00	2.00	2.00	5.00	5.00
78	3.00	5.00	2.00	2.00	2.00	5.00	5.00
79	3.00	5.00	2.00	3.00	4.00	4.00	3.00
80	3.00	3.00	2.00	3.00	2.00	4.00	5.00
81	5.00	4.00	2.00	5.00	4.00	2.00	4.00
82	3.00	5.00	2.00	2.00	2.00	5.00	5.00
83	3.00	5.00	2.00	2.00	2.00	5.00	5.00
84	3.00	5.00	2.00	3.00	4.00	4.00	3.00
85	3.00	3.00	2.00	3.00	2.00	4.00	5.00
86	5.00	4.00	2.00	5.00	4.00	2.00	4.00
87	3.00	5.00	2.00	2.00	2.00	5.00	5.00
88	3.00	5.00	2.00	2.00	2.00	5.00	5.00
89	3.00	5.00	2.00	3.00	4.00	4.00	3.00
90	3.00	5.00	2.00	2.00	2.00	5.00	5.00
91	3.00	5.00	2.00	3.00	4.00	4.00	3.00
92	3.00	3.00	2.00	3.00	2.00	4.00	5.00
93	5.00	4.00	2.00	5.00	4.00	2.00	4.00
94	3.00	5.00	2.00	2.00	2.00	5.00	5.00
95	3.00	5.00	2.00	2.00	2.00	5.00	5.00
96	3.00	5.00	2.00	3.00	4.00	4.00	3.00
97	3.00	5.00	2.00	2.00	2.00	5.00	5.00
98	3.00	5.00	2.00	3.00	4.00	4.00	3.00
99	3.00	3.00	2.00	3.00	2.00	4.00	5.00
100	5.00	4.00	2.00	5.00	4.00	2.00	4.00

	يقاوم	تناسب	التدريب	الخبراء	تصميم	عنبعد	تنسيقاً
51	4.00	3.00	3.00	1.00	1.00	1.00	2.00
52	4.00	3.00	3.00	1.00	1.00	1.00	2.00
53	4.00	3.00	3.00	1.00	1.00	1.00	2.00
54	4.00	3.00	3.00	1.00	1.00	1.00	2.00
55	4.00	3.00	3.00	1.00	1.00	1.00	3.00
56	4.00	3.00	3.00	1.00	1.00	1.00	3.00
57	4.00	3.00	4.00	3.00	2.00	2.00	1.00
58	4.00	4.00	4.00	5.00	5.00	4.00	4.00
59	4.00	3.00	4.00	3.00	2.00	2.00	1.00
60	4.00	2.00	2.00	2.00	4.00	2.00	1.00
61	4.00	2.00	2.00	2.00	4.00	2.00	1.00
62	4.00	3.00	4.00	3.00	2.00	2.00	1.00
63	4.00	4.00	4.00	5.00	5.00	4.00	4.00
64	4.00	3.00	4.00	3.00	2.00	2.00	1.00
65	4.00	3.00	4.00	3.00	2.00	2.00	1.00
66	4.00	3.00	4.00	3.00	2.00	2.00	1.00
67	4.00	3.00	4.00	3.00	3.00	2.00	1.00
68	4.00	4.00	4.00	5.00	5.00	4.00	4.00
69	3.00	4.00	4.00	4.00	4.00	4.00	2.00
70	5.00	4.00	5.00	5.00	2.00	2.00	2.00
71	3.00	5.00	5.00	5.00	2.00	2.00	2.00
72	5.00	4.00	5.00	5.00	3.00	2.00	2.00
73	5.00	4.00	5.00	5.00	2.00	2.00	2.00
74	3.00	4.00	4.00	4.00	4.00	4.00	2.00
75	5.00	4.00	5.00	5.00	2.00	2.00	2.00
76	3.00	5.00	5.00	5.00	2.00	2.00	2.00
77	5.00	4.00	5.00	5.00	3.00	2.00	2.00
78	5.00	4.00	5.00	5.00	2.00	2.00	2.00
79	3.00	4.00	4.00	4.00	4.00	4.00	2.00
80	5.00	4.00	5.00	5.00	2.00	2.00	2.00
81	3.00	5.00	5.00	5.00	2.00	2.00	2.00
82	5.00	4.00	5.00	5.00	3.00	2.00	2.00
83	5.00	4.00	5.00	5.00	2.00	2.00	2.00
84	3.00	4.00	4.00	4.00	4.00	4.00	2.00
85	5.00	4.00	5.00	5.00	2.00	2.00	2.00
86	3.00	5.00	5.00	5.00	2.00	2.00	2.00
87	5.00	4.00	5.00	5.00	3.00	2.00	2.00
88	5.00	4.00	5.00	5.00	2.00	2.00	2.00
89	3.00	4.00	4.00	4.00	4.00	4.00	2.00
90	5.00	4.00	5.00	5.00	2.00	2.00	2.00
91	3.00	4.00	4.00	4.00	4.00	4.00	2.00
92	5.00	4.00	5.00	5.00	2.00	2.00	2.00
93	3.00	5.00	5.00	5.00	2.00	2.00	2.00
94	5.00	4.00	5.00	5.00	2.00	2.00	2.00
95	5.00	4.00	5.00	5.00	2.00	2.00	2.00
96	3.00	4.00	4.00	4.00	4.00	4.00	2.00
97	5.00	4.00	5.00	5.00	2.00	2.00	2.00
98	3.00	4.00	4.00	4.00	4.00	4.00	2.00
99	5.00	4.00	5.00	5.00	2.00	2.00	2.00
100	3.00	5.00	5.00	5.00	2.00	2.00	2.00

أشتراك	التوعية	اهمية	معاهد	المختصين	مناسب	تنسيقنم	
2	1.00	5.00	.	.	.	3.00	51
2	5.00	5.00	.	.	.	3.00	52
2	5.00	5.00	.	.	.	3.00	53
2	1.00	5.00	.	.	.	3.00	54
2	2.00	5.00	.	.	.	3.00	55
2	1.00	4.00	.	.	.	3.00	56
1	1.00	3.00	.	.	.	3.00	57
1	4.00	5.00	.	.	.	2.00	58
2	4.00	5.00	.	.	.	3.00	59
2	2.00	5.00	.	.	.	4.00	60
1	5.00	5.00	.	.	.	4.00	61
2	4.00	5.00	.	.	.	3.00	62
1	4.00	5.00	.	.	.	2.00	63
1	4.00	5.00	.	.	.	3.00	64
1	2.00	5.00	.	.	.	3.00	65
1	2.00	5.00	.	.	.	3.00	66
1	4.00	5.00	.	.	.	3.00	67
1	5.00	5.00	.	.	.	2.00	68
.	.	.	2.00	1.00	3.00	3.00	69
.	.	.	2.00	2.00	2.00	3.00	70
.	.	.	3.00	1.00	3.00	3.00	71
.	.	.	3.00	2.00	3.00	3.00	72
.	.	.	3.00	2.00	3.00	3.00	73
.	.	.	3.00	2.00	3.00	3.00	74
.	.	.	3.00	3.00	3.00	3.00	75
.	.	.	3.00	3.00	3.00	3.00	76
.	.	.	3.00	3.00	3.00	3.00	77
.	.	.	3.00	3.00	3.00	3.00	78
.	.	.	2.00	2.00	2.00	3.00	79
.	.	.	3.00	1.00	3.00	3.00	80
.	.	.	3.00	3.00	2.00	3.00	81
.	.	.	2.00	3.00	3.00	3.00	82
.	.	.	3.00	3.00	3.00	3.00	83
.	.	.	3.00	3.00	3.00	3.00	84
.	.	.	3.00	1.00	2.00	3.00	85
.	.	.	3.00	1.00	3.00	3.00	86
.	.	.	3.00	2.00	3.00	3.00	87
.	.	.	3.00	3.00	3.00	3.00	88
.	.	.	3.00	3.00	3.00	3.00	89
.	.	.	3.00	3.00	3.00	3.00	90
.	.	.	3.00	3.00	3.00	3.00	91
.	.	.	3.00	3.00	3.00	3.00	92
.	.	.	3.00	3.00	3.00	3.00	93
.	.	.	3.00	3.00	3.00	3.00	94
.	.	.	2.00	3.00	2.00	3.00	95
.	.	.	3.00	3.00	3.00	3.00	96
.	.	.	3.00	3.00	3.00	3.00	97
.	.	.	3.00	3.00	3.00	3.00	98
.	.	.	2.00	3.00	3.00	3.00	99
.	.	.	3.00	3.00	3.00	3.00	100

	المهارة	المعرفة	المقدرة	بأساليب	الإثبات	الدوري	الزام
51	.	.	.	.	.	1.00	5.00
52	.	.	.	.	.	1.00	4.00
53	.	.	.	.	.	1.00	3.00
54	.	.	.	.	.	1.00	2.00
55	.	.	.	.	.	1.00	4.00
56	.	.	.	.	.	1.00	3.00
57	.	.	.	.	.	1.00	5.00
58	.	.	.	.	.	3.00	3.00
59	.	.	.	.	.	3.00	4.00
60	.	.	.	.	.	5.00	4.00
61	.	.	.	.	.	5.00	4.00
62	.	.	.	.	.	3.00	4.00
63	.	.	.	.	.	3.00	3.00
64	.	.	.	.	.	3.00	4.00
65	.	.	.	.	.	3.00	4.00
66	.	.	.	.	.	3.00	4.00
67	.	.	.	.	.	3.00	4.00
68	.	.	.	.	.	3.00	3.00
69	5.00	4.00	4.00	4.00	4.00	.	.
70	4.00	5.00	5.00	3.00	4.00	.	.
71	4.00	3.00	3.00	4.00	3.00	.	.
72	5.00	5.00	4.00	2.00	3.00	.	.
73	4.00	3.00	3.00	3.00	4.00	.	.
74	3.00	3.00	3.00	3.00	3.00	.	.
75	3.00	2.00	2.00	2.00	2.00	.	.
76	3.00	2.00	4.00	2.00	3.00	.	.
77	1.00	2.00	3.00	2.00	3.00	.	.
78	3.00	2.00	3.00	1.00	3.00	.	.
79	3.00	2.00	2.00	2.00	3.00	.	.
80	2.00	2.00	2.00	2.00	2.00	.	.
81	4.00	2.00	4.00	2.00	2.00	.	.
82	4.00	4.00	4.00	2.00	3.00	.	.
83	4.00	4.00	2.00	2.00	2.00	.	.
84	1.00	1.00	1.00	1.00	1.00	.	.
85	2.00	2.00	4.00	3.00	2.00	.	.
86	2.00	2.00	3.00	2.00	3.00	.	.
87	2.00	3.00	4.00	2.00	3.00	.	.
88	4.00	2.00	4.00	2.00	3.00	.	.
89	2.00	2.00	4.00	2.00	2.00	.	.
90	2.00	2.00	3.00	2.00	2.00	.	.
91	3.00	2.00	2.00	2.00	3.00	.	.
92	3.00	2.00	4.00	2.00	2.00	.	.
93	2.00	2.00	3.00	2.00	2.00	.	.
94	3.00	2.00	3.00	4.00	2.00	.	.
95	4.00	2.00	3.00	2.00	4.00	.	.
96	2.00	2.00	4.00	3.00	2.00	.	.
97	3.00	2.00	3.00	2.00	2.00	.	.
98	2.00	2.00	3.00	3.00	2.00	.	.
99	5.00	1.00	2.00	2.00	3.00	.	.
100	2.00	2.00	4.00	3.00	2.00	.	.

	الحوافز	توزيع	التزكية	المصرح	بصمة	محركات	لصيانة
51	1.00	4.00	4.00	4.00	1.00	1.00	3.00
52	3.00	4.00	4.00	3.00	1.00	1.00	3.00
53	1.00	4.00	4.00	3.00	1.00	1.00	3.00
54	1.00	4.00	4.00	4.00	1.00	1.00	3.00
55	1.00	4.00	4.00	3.00	3.00	1.00	3.00
56	1.00	4.00	4.00	4.00	2.00	1.00	3.00
57	1.00	4.00	4.00	4.00	4.00	3.00	5.00
58	2.00	5.00	2.00	3.00	4.00	1.00	4.00
59	2.00	4.00	4.00	4.00	5.00	3.00	5.00
60	3.00	4.00	5.00	4.00	4.00	4.00	4.00
61	3.00	4.00	5.00	4.00	5.00	4.00	4.00
62	2.00	4.00	4.00	4.00	4.00	3.00	5.00
63	2.00	5.00	2.00	2.00	4.00	1.00	4.00
64	2.00	4.00	4.00	4.00	4.00	3.00	5.00
65	2.00	4.00	4.00	4.00	4.00	3.00	5.00
66	2.00	4.00	4.00	4.00	5.00	3.00	5.00
67	2.00	4.00	4.00	4.00	4.00	3.00	5.00
68	2.00	5.00	2.00	5.00	4.00	1.00	4.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	الأحتياط	تحديثها	المدة	المزامنة	تلائم	باستمرار	التقدم
51	3.00	2.00	4.00	3.00	5.00	2.00	2.00
52	3.00	2.00	1.00	1.00	5.00	3.00	2.00
53	3.00	2.00	2.00	1.00	4.00	2.00	2.00
54	3.00	2.00	3.00	3.00	3.00	2.00	2.00
55	3.00	2.00	2.00	3.00	2.00	2.00	2.00
56	3.00	2.00	2.00	2.00	2.00	3.00	2.00
57	5.00	5.00	4.00	5.00	4.00	1.00	3.00
58	5.00	5.00	3.00	2.00	2.00	2.00	2.00
59	5.00	4.00	4.00	3.00	4.00	2.00	4.00
60	4.00	5.00	4.00	3.00	4.00	1.00	3.00
61	4.00	5.00	4.00	3.00	4.00	1.00	3.00
62	5.00	5.00	4.00	5.00	4.00	4.00	2.00
63	5.00	5.00	3.00	2.00	2.00	5.00	4.00
64	5.00	5.00	4.00	5.00	4.00	4.00	4.00
65	5.00	5.00	4.00	5.00	4.00	4.00	3.00
66	5.00	5.00	4.00	5.00	4.00	4.00	2.00
67	5.00	5.00	4.00	5.00	4.00	4.00	3.00
68	5.00	5.00	3.00	2.00	2.00	5.00	2.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	تشكيل	رصد	التتبع	ربط	ضوابطتشغ	ضوابطعمل	ظوابطقاع
51	2.00	1.00	4.00	3.00	2.00	4.00	3.00
52	2.00	3.00	2.00	3.00	4.00	3.00	3.00
53	3.00	1.00	2.00	3.00	3.00	4.00	4.00
54	1.00	1.00	3.00	2.00	4.00	2.00	4.00
55	4.00	3.00	4.00	3.00	4.00	4.00	4.00
56	2.00	3.00	3.00	3.00	4.00	4.00	4.00
57	5.00	2.00	5.00	4.00	5.00	4.00	1.00
58	2.00	3.00	4.00	1.00	4.00	3.00	4.00
59	4.00	4.00	4.00	4.00	4.00	2.00	4.00
60	3.00	5.00	4.00	2.00	4.00	4.00	1.00
61	5.00	2.00	5.00	3.00	2.00	4.00	1.00
62	4.00	2.00	4.00	4.00	4.00	4.00	4.00
63	2.00	3.00	4.00	1.00	4.00	3.00	4.00
64	4.00	4.00	4.00	4.00	4.00	4.00	4.00
65	4.00	4.00	4.00	2.00	4.00	4.00	4.00
66	4.00	4.00	4.00	4.00	4.00	4.00	4.00
67	4.00	4.00	4.00	3.00	4.00	4.00	4.00
68	2.00	3.00	4.00	1.00	4.00	3.00	4.00
69	.	.	.	.	.	.	.
70	.	.	.	.	.	.	.
71	.	.	.	.	.	.	.
72	.	.	.	.	.	.	.
73	.	.	.	.	.	.	.
74	.	.	.	.	.	.	.
75	.	.	.	.	.	.	.
76	.	.	.	.	.	.	.
77	.	.	.	.	.	.	.
78	.	.	.	.	.	.	.
79	.	.	.	.	.	.	.
80	.	.	.	.	.	.	.
81	.	.	.	.	.	.	.
82	.	.	.	.	.	.	.
83	.	.	.	.	.	.	.
84	.	.	.	.	.	.	.
85	.	.	.	.	.	.	.
86	.	.	.	.	.	.	.
87	.	.	.	.	.	.	.
88	.	.	.	.	.	.	.
89	.	.	.	.	.	.	.
90	.	.	.	.	.	.	.
91	.	.	.	.	.	.	.
92	.	.	.	.	.	.	.
93	.	.	.	.	.	.	.
94	.	.	.	.	.	.	.
95	.	.	.	.	.	.	.
96	.	.	.	.	.	.	.
97	.	.	.	.	.	.	.
98	.	.	.	.	.	.	.
99	.	.	.	.	.	.	.
100	.	.	.	.	.	.	.

	ظوابطشبك	ضوابطالد	البشري	المكاني	المطورة	الجاهزة	الانترنت
51	4.00	2.00	4.00	5.00	4.00	4.00	4.00
52	3.00	4.00	4.00	4.00	3.00	4.00	4.00
53	1.00	4.00	4.00	4.00	4.00	4.00	4.00
54	3.00	4.00	4.00	3.00	2.00	5.00	4.00
55	3.00	4.00	4.00	5.00	4.00	4.00	4.00
56	2.00	4.00	4.00	5.00	4.00	4.00	4.00
57	3.00	4.00	5.00	5.00	4.00	4.00	4.00
58	4.00	4.00	5.00	4.00	5.00	5.00	3.00
59	4.00	4.00	5.00	4.00	5.00	4.00	5.00
60	3.00	5.00	5.00	4.00	4.00	5.00	4.00
61	3.00	5.00	5.00	4.00	4.00	5.00	4.00
62	4.00	4.00	5.00	4.00	5.00	5.00	5.00
63	3.00	4.00	5.00	4.00	5.00	5.00	3.00
64	3.00	4.00	5.00	5.00	5.00	3.00	5.00
65	4.00	4.00	5.00	5.00	5.00	3.00	5.00
66	3.00	4.00	5.00	5.00	5.00	3.00	5.00
67	4.00	4.00	5.00	5.00	5.00	4.00	5.00
68	3.00	4.00	5.00	5.00	5.00	5.00	3.00
69	.	.	3.00	5.00	5.00	4.00	4.00
70	.	.	4.00	5.00	4.00	3.00	5.00
71	.	.	5.00	5.00	4.00	4.00	5.00
72	.	.	5.00	5.00	4.00	4.00	5.00
73	.	.	5.00	5.00	5.00	4.00	5.00
74	.	.	3.00	5.00	5.00	4.00	4.00
75	.	.	4.00	5.00	4.00	3.00	5.00
76	.	.	5.00	5.00	4.00	4.00	5.00
77	.	.	5.00	5.00	4.00	4.00	5.00
78	.	.	5.00	5.00	5.00	4.00	5.00
79	.	.	3.00	5.00	5.00	4.00	4.00
80	.	.	4.00	5.00	4.00	3.00	5.00
81	.	.	5.00	5.00	4.00	4.00	5.00
82	.	.	5.00	5.00	4.00	4.00	5.00
83	.	.	5.00	4.00	5.00	4.00	5.00
84	.	.	3.00	5.00	5.00	4.00	4.00
85	.	.	4.00	5.00	4.00	3.00	5.00
86	.	.	5.00	4.00	4.00	4.00	5.00
87	.	.	5.00	4.00	4.00	4.00	5.00
88	.	.	5.00	4.00	5.00	4.00	5.00
89	.	.	3.00	4.00	5.00	4.00	4.00
90	.	.	5.00	4.00	5.00	4.00	5.00
91	.	.	3.00	4.00	5.00	4.00	4.00
92	.	.	4.00	4.00	4.00	3.00	5.00
93	.	.	5.00	2.00	4.00	4.00	5.00
94	.	.	5.00	4.00	4.00	4.00	5.00
95	.	.	5.00	4.00	5.00	4.00	5.00
96	.	.	3.00	5.00	5.00	4.00	4.00
97	.	.	5.00	5.00	5.00	4.00	5.00
98	.	.	3.00	5.00	5.00	4.00	4.00
99	.	.	4.00	5.00	4.00	3.00	5.00
100	.	.	5.00	5.00	4.00	4.00	5.00

	الخدمات	احترازات	وسائط	منافسين	السياسة	التشريعا	المجرمين
51	3.00	3.00	3.00	1.00	5.00	5.00	5.00
52	3.00	3.00	3.00	1.00	5.00	5.00	5.00
53	3.00	3.00	3.00	1.00	5.00	5.00	5.00
54	3.00	3.00	3.00	1.00	5.00	5.00	5.00
55	3.00	3.00	3.00	1.00	5.00	5.00	5.00
56	3.00	3.00	3.00	1.00	5.00	5.00	5.00
57	5.00	5.00	5.00	5.00	5.00	5.00	5.00
58	4.00	4.00	4.00	5.00	5.00	4.00	4.00
59	5.00	5.00	5.00	5.00	5.00	5.00	5.00
60	5.00	5.00	5.00	3.00	5.00	4.00	4.00
61	5.00	5.00	5.00	3.00	5.00	4.00	4.00
62	5.00	5.00	5.00	5.00	5.00	5.00	5.00
63	4.00	4.00	4.00	5.00	5.00	4.00	4.00
64	5.00	5.00	5.00	5.00	5.00	5.00	5.00
65	5.00	5.00	5.00	5.00	5.00	5.00	5.00
66	5.00	5.00	5.00	5.00	5.00	5.00	5.00
67	5.00	5.00	5.00	5.00	5.00	5.00	5.00
68	4.00	4.00	4.00	5.00	5.00	4.00	4.00
69	4.00	3.00	4.00	4.00	5.00	5.00	5.00
70	4.00	4.00	4.00	4.00	5.00	5.00	5.00
71	4.00	4.00	4.00	4.00	5.00	5.00	5.00
72	4.00	4.00	4.00	4.00	5.00	5.00	5.00
73	4.00	4.00	4.00	4.00	5.00	5.00	5.00
74	4.00	3.00	4.00	4.00	5.00	5.00	5.00
75	4.00	4.00	4.00	4.00	5.00	5.00	5.00
76	4.00	4.00	4.00	4.00	5.00	5.00	5.00
77	4.00	4.00	4.00	4.00	5.00	5.00	5.00
78	4.00	4.00	4.00	4.00	5.00	5.00	5.00
79	4.00	3.00	4.00	4.00	5.00	5.00	5.00
80	4.00	4.00	4.00	4.00	5.00	5.00	5.00
81	4.00	4.00	4.00	4.00	5.00	5.00	5.00
82	4.00	4.00	4.00	4.00	5.00	5.00	5.00
83	4.00	4.00	4.00	4.00	5.00	5.00	5.00
84	4.00	3.00	4.00	4.00	5.00	5.00	5.00
85	4.00	4.00	4.00	4.00	5.00	5.00	5.00
86	4.00	4.00	4.00	4.00	5.00	5.00	5.00
87	4.00	4.00	4.00	4.00	5.00	5.00	5.00
88	4.00	4.00	4.00	4.00	5.00	5.00	5.00
89	4.00	3.00	4.00	4.00	5.00	5.00	5.00
90	4.00	4.00	4.00	4.00	5.00	5.00	5.00
91	4.00	3.00	4.00	4.00	5.00	5.00	5.00
92	4.00	4.00	4.00	4.00	5.00	5.00	5.00
93	4.00	4.00	4.00	4.00	5.00	5.00	5.00
94	4.00	4.00	3.00	4.00	5.00	5.00	5.00
95	4.00	4.00	3.00	4.00	5.00	5.00	5.00
96	4.00	3.00	3.00	4.00	5.00	5.00	5.00
97	4.00	4.00	3.00	4.00	5.00	5.00	5.00
98	3.00	3.00	3.00	4.00	5.00	5.00	5.00
99	4.00	4.00	3.00	4.00	5.00	5.00	5.00
100	4.00	2.00	3.00	4.00	5.00	5.00	5.00

	الرؤساء	عقوبات	أعلان	lev_1	العينةz	zsc001	المطورةz
51	4.00	5.00	4.00	1.00	-.93157	-.93157	-.05569
52	4.00	5.00	4.00	1.00	-.93157	-.93157	-1.36437
53	4.00	5.00	3.00	.41	-.93157	-.93157	-.05569
54	4.00	5.00	4.00	1.00	-.93157	-.93157	-2.67305
55	4.00	5.00	5.00	.42	-.93157	-.93157	-.05569
56	4.00	5.00	5.00	.05	-.93157	-.93157	-.05569
57	5.00	5.00	5.00	.60	-.93157	-.93157	-.05569
58	4.00	5.00	5.00	.29	-.93157	-.93157	1.25299
59	5.00	5.00	5.00	.21	-.93157	-.93157	1.25299
60	5.00	4.00	5.00	.19	-.93157	-.93157	-.05569
61	4.00	4.00	5.00	.34	-.93157	-.93157	-.05569
62	4.00	5.00	5.00	.18	-.93157	-.93157	1.25299
63	4.00	5.00	5.00	.29	-.93157	-.93157	1.25299
64	4.00	5.00	5.00	.20	-.93157	-.93157	1.25299
65	4.00	5.00	5.00	.20	-.93157	-.93157	1.25299
66	4.00	5.00	5.00	.21	-.93157	-.93157	1.25299
67	5.00	5.00	5.00	.24	-.93157	-.93157	1.25299
68	4.00	5.00	5.00	.29	-.93157	-.93157	1.25299
69	5.00	5.00	5.00	.24	.26253	.26253	1.25299
70	5.00	5.00	5.00	.24	.26253	.26253	-.05569
71	5.00	5.00	5.00	.24	.26253	.26253	-.05569
72	5.00	5.00	5.00	.24	.26253	.26253	-.05569
73	5.00	5.00	5.00	.24	.26253	.26253	1.25299
74	5.00	5.00	5.00	.24	.26253	.26253	1.25299
75	5.00	5.00	5.00	.24	.26253	.26253	-.05569
76	5.00	5.00	5.00	.24	.26253	.26253	-.05569
77	5.00	5.00	5.00	.24	.26253	.26253	-.05569
78	5.00	5.00	5.00	.24	.26253	.26253	1.25299
79	5.00	5.00	5.00	.24	.26253	.26253	1.25299
80	5.00	5.00	5.00	.24	.26253	.26253	-.05569
81	5.00	5.00	5.00	.24	.26253	.26253	-.05569
82	5.00	5.00	5.00	.24	.26253	.26253	-.05569
83	5.00	5.00	5.00	.24	.26253	.26253	1.25299
84	5.00	5.00	5.00	.24	.26253	.26253	1.25299
85	3.00	5.00	5.00	.24	.26253	.26253	-.05569
86	5.00	5.00	5.00	.24	.26253	.26253	-.05569
87	5.00	5.00	5.00	.24	.26253	.26253	-.05569
88	3.00	5.00	5.00	.24	.26253	.26253	1.25299
89	5.00	5.00	5.00	.24	.26253	.26253	1.25299
90	5.00	5.00	5.00	.24	.26253	.26253	1.25299
91	3.00	5.00	5.00	.24	.26253	.26253	1.25299
92	5.00	5.00	5.00	.24	.26253	.26253	-.05569
93	5.00	5.00	5.00	.24	.26253	.26253	-.05569
94	5.00	5.00	5.00	.24	.26253	.26253	-.05569
95	5.00	5.00	5.00	.24	.26253	.26253	1.25299
96	5.00	5.00	5.00	.24	.26253	.26253	1.25299
97	5.00	5.00	5.00	.24	.26253	.26253	1.25299
98	5.00	5.00	5.00	.24	.26253	.26253	1.25299
99	5.00	5.00	5.00	.24	.26253	.26253	-.05569
100	5.00	5.00	5.00	.24	.26253	.26253	-.05569

	الجاهزةz	الانترنz	الخدماتz	احترازاz	وسائطz	منافسينz
51	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
52	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
53	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
54	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
55	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
56	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
57	-.63907	-.84900	1.47876	1.50430	1.36437	1.19422
58	.72622	-2.53504	.17560	.24176	.05569	1.19422
59	-.63907	.83704	1.47876	1.50430	1.36437	1.19422
60	.72622	-.84900	1.47876	1.50430	1.36437	-.17476
61	.72622	-.84900	1.47876	1.50430	1.36437	-.17476
62	.72622	.83704	1.47876	1.50430	1.36437	1.19422
63	.72622	-2.53504	.17560	.24176	.05569	1.19422
64	-2.00437	.83704	1.47876	1.50430	1.36437	1.19422
65	-2.00437	.83704	1.47876	1.50430	1.36437	1.19422
66	-2.00437	.83704	1.47876	1.50430	1.36437	1.19422
67	-.63907	.83704	1.47876	1.50430	1.36437	1.19422
68	.72622	-2.53504	.17560	.24176	.05569	1.19422
69	-.63907	-.84900	.17560	-1.02077	.05569	.50973
70	-2.00437	.83704	.17560	.24176	.05569	.50973
71	-.63907	.83704	.17560	.24176	.05569	.50973
72	-.63907	.83704	.17560	.24176	.05569	.50973
73	-.63907	.83704	.17560	.24176	.05569	.50973
74	-.63907	-.84900	.17560	-1.02077	.05569	.50973
75	-2.00437	.83704	.17560	.24176	.05569	.50973
76	-.63907	.83704	.17560	.24176	.05569	.50973
77	-.63907	.83704	.17560	.24176	.05569	.50973
78	-.63907	.83704	.17560	.24176	.05569	.50973
79	-.63907	-.84900	.17560	-1.02077	.05569	.50973
80	-2.00437	.83704	.17560	.24176	.05569	.50973
81	-.63907	.83704	.17560	.24176	.05569	.50973
82	-.63907	.83704	.17560	.24176	.05569	.50973
83	-.63907	.83704	.17560	.24176	.05569	.50973
84	-.63907	-.84900	.17560	-1.02077	.05569	.50973
85	-2.00437	.83704	.17560	.24176	.05569	.50973
86	-.63907	.83704	.17560	.24176	.05569	.50973
87	-.63907	.83704	.17560	.24176	.05569	.50973
88	-.63907	.83704	.17560	.24176	.05569	.50973
89	-.63907	-.84900	.17560	-1.02077	.05569	.50973
90	-.63907	.83704	.17560	.24176	.05569	.50973
91	-.63907	-.84900	.17560	-1.02077	.05569	.50973
92	-2.00437	.83704	.17560	.24176	.05569	.50973
93	-.63907	.83704	.17560	.24176	.05569	.50973
94	-.63907	.83704	.17560	.24176	-1.25299	.50973
95	-.63907	.83704	.17560	.24176	-1.25299	.50973
96	-.63907	-.84900	.17560	-1.02077	-1.25299	.50973
97	-.63907	.83704	.17560	.24176	-1.25299	.50973
98	-.63907	-.84900	-1.12755	-1.02077	-1.25299	.50973
99	-2.00437	.83704	.17560	.24176	-1.25299	.50973
100	-.63907	.83704	.17560	-2.28331	-1.25299	.50973

	العينة	الوظيفة	المؤسسة	v3	الأنترنت	الاسلوب	مصروفات
101	2.00	.	.	.	.	.	.
102	2.00	.	.	.	.	.	.
103	2.00	.	.	.	.	.	.
104	2.00	.	.	.	.	.	.
105	3.00	.	.	.	.	.	.
106	3.00	.	.	.	.	.	.
107	3.00	.	.	.	.	.	.
108	3.00	.	.	.	.	.	.
109	3.00	.	.	.	.	.	.
110	3.00	.	.	.	.	.	.
111	3.00	.	.	.	.	.	.
112	3.00	.	.	.	.	.	.
113	3.00	.	.	.	.	.	.
114	3.00	.	.	.	.	.	.
115	3.00	.	.	.	.	.	.
116	3.00	.	.	.	.	.	.
117	3.00	.	.	.	.	.	.
118	3.00	.	.	.	.	.	.
119	3.00	.	.	.	.	.	.
120	3.00	.	.	.	.	.	.
121	3.00	.	.	.	.	.	.
122	3.00	.	.	.	.	.	.
123	3.00	.	.	.	.	.	.
124	3.00	.	.	.	.	.	.
125	3.00	.	.	.	.	.	.
126	3.00	.	.	.	.	.	.
127	3.00	.	.	.	.	.	.
128	3.00	.	.	.	.	.	.
129	3.00	.	.	.	.	.	.
130	3.00	.	.	.	.	.	.
131	3.00	.	.	.	.	.	.
132	3.00	.	.	.	.	.	.
133	3.00	.	.	.	.	.	.
134	3.00	.	.	.	.	.	.
135	3.00	.	.	.	.	.	.
136	3.00	.	.	.	.	.	.
137	3.00	.	.	.	.	.	.
138	3.00	.	.	.	.	.	.
139	3.00	.	.	.	.	.	.
140	3.00	.	.	.	.	.	.
141	3.00	.	.	.	.	.	.

	قسم	العاملين	سياسة	حدوث	v11	v12	v13
101	.	.	.	.	5	5	2
102	.	.	.	.	5	5	2
103	.	.	.	.	4	3	4
104	.	.	.	.	4	5	2
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	v14	v15	v16	v17	v18	v19	v20
101	2	3	4	2	2	3	3
102	4	3	4	2	2	3	3
103	2	5	4	4	4	3	2
104	2	3	4	2	2	3	3
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	v21	التلاعب	البرامج	البيانات	تدمير	تعطيل	تنصت
101	2	3	3	3.00	3	4	4
102	2	3	3	3.00	3	4	4
103	2	3	4	3.00	3	4	4
104	2	5	4	3.00	4	4	3
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	نسخ	برامجها	استيلاء	أحصنة	فيروسات	أختراقات	إعتراض
101	4	5	3	4	4	4	3
102	4	5	3	4	4	4	3
103	4	5	3	4	4	4	3
104	3	5	3	4	4	4	3
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	إغراق	أفشاء	محاولة	فك	lan	الأقرص	wan
101	3	.	.	.	.	.	.
102	3	.	.	.	.	.	.
103	3	.	.	.	.	.	.
104	5	.	.	.	.	.	.
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	internet	vpn	عسكرية	إبراز	تجارية	تسلية	انتقام
101	.	.	4.00	3.00	4.00	5.00	4.00
102	.	.	4.00	4.00	4.00	5.00	5.00
103	.	.	4.00	5.00	4.00	5.00	5.00
104	.	.	3.00	5.00	4.00	4.00	4.00
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	الشخصية	التكلفة	الإنذرات	الضعف	فيروس	طروادة	spoofing
101	5.00	.	.	.	.	.	.
102	5.00	.	.	.	.	.	.
103	3.00	.	.	.	.	.	.
104	5.00	.	.	.	.	.	.
105	.	.	.	4.000	5.00	5.00	4.00
106	.	.	.	5.000	5.00	4.00	5.00
107	.	.	.	5.000	5.00	4.00	3.00
108	.	.	.	4.000	5.00	5.00	4.00
109	.	.	.	4.000	5.00	5.00	4.00
110	.	.	.	4.000	5.00	5.00	4.00
111	.	.	.	2.000	5.00	3.00	3.00
112	.	.	.	4.000	5.00	5.00	4.00
113	.	.	.	4.000	5.00	5.00	4.00
114	.	.	.	5.000	5.00	4.00	3.00
115	.	.	.	5.000	5.00	4.00	5.00
116	.	.	.	2.000	5.00	3.00	3.00
117	.	.	.	2.000	5.00	3.00	3.00
118	.	.	.	5.000	5.00	4.00	3.00
119	.	.	.	5.000	5.00	4.00	5.00
120	.	.	.	5.000	5.00	4.00	3.00
121	.	.	.	5.000	5.00	4.00	3.00
122	.	.	.	1.000	5.00	5.00	2.00
123	.	.	.	5.000	5.00	4.00	5.00
124	.	.	.	2.000	5.00	5.00	2.00
125	.	.	.	1.000	5.00	5.00	3.00
126	.	.	.	2.000	4.00	5.00	2.00
127	.	.	.	2.000	5.00	3.00	3.00
128	.	.	.	2.000	3.00	2.00	2.00
129	.	.	.	2.000	3.00	3.00	4.00
130	.	.	.	5.000	5.00	4.00	5.00
131	.	.	.	2.000	3.00	2.00	2.00
132	.	.	.	1.000	2.00	5.00	4.00
133	.	.	.	5.000	5.00	4.00	5.00
134	.	.	.	4.000	5.00	5.00	4.00
135	.	.	.	2.000	3.00	3.00	4.00
136	.	.	.	2.000	3.00	3.00	4.00
137	.	.	.	5.000	5.00	4.00	3.00
138	.	.	.	5.000	5.00	5.00	4.00
139	.	.	.	2.000	3.00	3.00	4.00
140	.	.	.	5.000	5.00	4.00	5.00
141	.	.	.	4.000	5.00	5.00	4.00

	انتحال	المنافذ	التشارك	الثغرات	ثغراتتح	برمجة	إرفاق
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	4.00	4.00	5.00	5.00	4.00	4.00	3.00
106	3.00	5.00	5.00	5.00	5.00	4.00	4.00
107	3.00	5.00	5.00	5.00	5.00	4.00	4.00
108	4.00	2.00	4.00	5.00	4.00	4.00	3.00
109	4.00	4.00	5.00	4.00	4.00	4.00	3.00
110	4.00	4.00	5.00	5.00	4.00	4.00	3.00
111	1.00	2.00	1.00	2.00	2.00	1.00	1.00
112	4.00	4.00	5.00	5.00	4.00	4.00	3.00
113	4.00	4.00	5.00	5.00	4.00	4.00	3.00
114	3.00	5.00	5.00	5.00	5.00	4.00	4.00
115	3.00	5.00	5.00	5.00	5.00	4.00	4.00
116	1.00	2.00	1.00	2.00	2.00	1.00	1.00
117	1.00	2.00	1.00	2.00	2.00	1.00	1.00
118	3.00	5.00	5.00	5.00	5.00	4.00	4.00
119	3.00	5.00	5.00	5.00	5.00	4.00	4.00
120	3.00	5.00	5.00	5.00	5.00	4.00	4.00
121	3.00	5.00	5.00	5.00	5.00	4.00	4.00
122	1.00	2.00	1.00	1.00	1.00	1.00	2.00
123	3.00	5.00	5.00	5.00	5.00	4.00	4.00
124	1.00	2.00	1.00	2.00	2.00	1.00	1.00
125	1.00	2.00	1.00	2.00	1.00	1.00	2.00
126	1.00	2.00	1.00	1.00	2.00	1.00	1.00
127	1.00	2.00	1.00	2.00	2.00	1.00	1.00
128	3.00	5.00	3.00	2.00	2.00	1.00	1.00
129	1.00	4.00	1.00	1.00	2.00	1.00	1.00
130	3.00	5.00	5.00	5.00	5.00	4.00	4.00
131	1.00	2.00	4.00	3.00	2.00	1.00	1.00
132	1.00	2.00	4.00	3.00	4.00	1.00	2.00
133	3.00	5.00	5.00	5.00	5.00	4.00	4.00
134	4.00	4.00	5.00	5.00	4.00	4.00	3.00
135	1.00	4.00	1.00	1.00	2.00	1.00	1.00
136	1.00	4.00	1.00	1.00	2.00	1.00	1.00
137	3.00	5.00	5.00	5.00	5.00	4.00	4.00
138	3.00	5.00	5.00	5.00	5.00	4.00	4.00
139	1.00	4.00	1.00	1.00	2.00	1.00	1.00
140	3.00	5.00	5.00	5.00	5.00	4.00	4.00
141	4.00	4.00	5.00	5.00	4.00	4.00	3.00

	التخفي	المزودات	السرقة	تشغيل	ترك	زراعة	القانوني
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	4.00	5.00	5.00	3.00	4.00	2.00	4.00
106	3.00	5.00	5.00	3.00	3.00	3.00	4.00
107	3.00	5.00	3.00	3.00	3.00	3.00	4.00
108	4.00	5.00	5.00	3.00	4.00	2.00	4.00
109	4.00	5.00	5.00	3.00	4.00	2.00	4.00
110	4.00	5.00	5.00	3.00	4.00	2.00	4.00
111	2.00	1.00	1.00	1.00	3.00	1.00	1.00
112	4.00	5.00	5.00	3.00	4.00	2.00	4.00
113	4.00	5.00	5.00	3.00	4.00	2.00	4.00
114	3.00	5.00	3.00	3.00	2.00	3.00	5.00
115	3.00	5.00	3.00	3.00	3.00	3.00	2.00
116	2.00	1.00	1.00	1.00	3.00	1.00	1.00
117	2.00	1.00	1.00	1.00	3.00	1.00	1.00
118	3.00	5.00	3.00	3.00	2.00	3.00	2.00
119	3.00	5.00	3.00	3.00	3.00	3.00	2.00
120	3.00	5.00	3.00	3.00	5.00	3.00	2.00
121	3.00	5.00	3.00	3.00	2.00	3.00	5.00
122	1.00	1.00	1.00	1.00	1.00	1.00	1.00
123	3.00	5.00	3.00	3.00	3.00	3.00	2.00
124	2.00	1.00	1.00	1.00	3.00	1.00	1.00
125	1.00	1.00	1.00	1.00	1.00	1.00	1.00
126	2.00	1.00	1.00	1.00	3.00	1.00	1.00
127	2.00	1.00	1.00	1.00	3.00	1.00	1.00
128	2.00	1.00	1.00	1.00	3.00	1.00	1.00
129	2.00	1.00	1.00	1.00	3.00	1.00	1.00
130	3.00	5.00	3.00	3.00	3.00	3.00	2.00
131	2.00	1.00	1.00	1.00	3.00	1.00	1.00
132	1.00	4.00	1.00	1.00	4.00	1.00	1.00
133	3.00	5.00	3.00	3.00	3.00	3.00	2.00
134	4.00	5.00	5.00	3.00	3.00	2.00	4.00
135	2.00	1.00	1.00	1.00	3.00	1.00	1.00
136	2.00	1.00	1.00	1.00	3.00	1.00	1.00
137	3.00	5.00	3.00	3.00	3.00	3.00	2.00
138	3.00	5.00	3.00	3.00	3.00	3.00	2.00
139	2.00	1.00	1.00	1.00	3.00	1.00	1.00
140	3.00	5.00	3.00	3.00	3.00	3.00	2.00
141	4.00	5.00	5.00	3.00	3.00	2.00	4.00

	الصيانة	مرخص	غمرخص	مجاني	غمجاني	cookies	groove
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	2.00	3.00	5.00	5.00	4.00	5.00	3.00
106	4.00	4.00	5.00	5.00	4.00	5.00	4.00
107	3.00	3.00	5.00	5.00	4.00	5.00	4.00
108	3.00	3.00	5.00	5.00	4.00	5.00	3.00
109	3.00	3.00	5.00	5.00	4.00	5.00	2.00
110	3.00	3.00	5.00	5.00	4.00	5.00	3.00
111	1.00	1.00	4.00	5.00	3.00	4.00	2.00
112	3.00	3.00	5.00	5.00	4.00	5.00	3.00
113	3.00	3.00	5.00	5.00	4.00	5.00	2.00
114	3.00	3.00	5.00	5.00	4.00	5.00	1.00
115	3.00	4.00	5.00	5.00	4.00	5.00	4.00
116	1.00	1.00	4.00	5.00	3.00	4.00	2.00
117	1.00	1.00	4.00	5.00	3.00	4.00	2.00
118	3.00	3.00	5.00	5.00	4.00	5.00	1.00
119	3.00	4.00	5.00	5.00	4.00	5.00	4.00
120	3.00	3.00	5.00	5.00	4.00	5.00	4.00
121	3.00	2.00	5.00	5.00	4.00	5.00	4.00
122	1.00	2.00	5.00	5.00	4.00	3.00	2.00
123	3.00	4.00	5.00	5.00	4.00	5.00	4.00
124	1.00	1.00	4.00	5.00	3.00	4.00	2.00
125	1.00	3.00	5.00	4.00	4.00	3.00	2.00
126	1.00	1.00	4.00	5.00	3.00	4.00	2.00
127	1.00	1.00	4.00	5.00	3.00	4.00	2.00
128	1.00	1.00	4.00	5.00	3.00	4.00	2.00
129	1.00	1.00	4.00	5.00	3.00	4.00	3.00
130	3.00	4.00	5.00	5.00	4.00	5.00	4.00
131	1.00	1.00	4.00	5.00	3.00	4.00	1.00
132	3.00	2.00	5.00	5.00	4.00	3.00	2.00
133	3.00	4.00	5.00	5.00	4.00	5.00	4.00
134	3.00	3.00	5.00	5.00	4.00	5.00	3.00
135	1.00	1.00	4.00	5.00	3.00	4.00	3.00
136	1.00	1.00	4.00	5.00	3.00	4.00	3.00
137	4.00	3.00	5.00	5.00	4.00	5.00	4.00
138	3.00	4.00	5.00	5.00	4.00	5.00	4.00
139	1.00	1.00	4.00	5.00	3.00	4.00	3.00
140	3.00	4.00	5.00	5.00	4.00	5.00	4.00
141	3.00	3.00	5.00	5.00	4.00	5.00	3.00

	caligula	netbus	subseven	hack	wincrash	tfn	toolkit
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	3.00	4.00	4.00	5.00	4.00	2.00	4.00
106	4.00	5.00	5.00	4.00	3.00	3.00	5.00
107	4.00	5.00	5.00	4.00	3.00	5.00	5.00
108	1.00	4.00	4.00	3.00	4.00	4.00	4.00
109	3.00	4.00	4.00	2.00	4.00	4.00	4.00
110	1.00	4.00	4.00	4.00	5.00	4.00	4.00
111	2.00	4.00	2.00	2.00	2.00	2.00	2.00
112	1.00	1.00	1.00	3.00	5.00	4.00	3.00
113	2.00	4.00	4.00	1.00	4.00	4.00	4.00
114	1.00	5.00	5.00	4.00	3.00	5.00	5.00
115	4.00	5.00	5.00	4.00	3.00	3.00	5.00
116	2.00	4.00	2.00	2.00	2.00	2.00	2.00
117	2.00	4.00	2.00	2.00	2.00	2.00	2.00
118	4.00	5.00	5.00	4.00	4.00	3.00	5.00
119	4.00	5.00	5.00	4.00	3.00	3.00	5.00
120	4.00	5.00	5.00	4.00	3.00	5.00	5.00
121	4.00	5.00	5.00	4.00	3.00	4.00	5.00
122	2.00	2.00	2.00	2.00	3.00	3.00	2.00
123	4.00	5.00	5.00	4.00	3.00	3.00	5.00
124	2.00	3.00	5.00	2.00	2.00	2.00	2.00
125	3.00	4.00	2.00	2.00	2.00	3.00	2.00
126	2.00	2.00	2.00	2.00	2.00	2.00	2.00
127	2.00	4.00	2.00	2.00	2.00	2.00	2.00
128	3.00	2.00	2.00	2.00	2.00	3.00	2.00
129	3.00	4.00	4.00	3.00	3.00	2.00	2.00
130	4.00	5.00	5.00	4.00	3.00	3.00	5.00
131	1.00	3.00	3.00	2.00	2.00	2.00	2.00
132	2.00	2.00	2.00	2.00	3.00	4.00	2.00
133	4.00	5.00	5.00	4.00	3.00	3.00	5.00
134	3.00	4.00	4.00	5.00	4.00	2.00	4.00
135	3.00	4.00	4.00	3.00	3.00	2.00	2.00
136	3.00	4.00	4.00	3.00	3.00	2.00	2.00
137	4.00	5.00	5.00	4.00	3.00	3.00	5.00
138	4.00	5.00	5.00	4.00	3.00	3.00	3.00
139	3.00	4.00	4.00	3.00	3.00	2.00	2.00
140	4.00	5.00	5.00	4.00	3.00	3.00	5.00
141	3.00	4.00	4.00	5.00	4.00	2.00	4.00

	msword	msexcel	revelat	icq	بتنصت	بالتغيل	المشاركة
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	4.00	4.00	3.00	3.00	3.00	3.00	5.00
106	4.00	4.00	2.00	5.00	4.00	4.00	4.00
107	4.00	4.00	4.00	5.00	4.00	4.00	4.00
108	4.00	4.00	3.00	3.00	3.00	3.00	4.00
109	5.00	5.00	3.00	3.00	3.00	3.00	5.00
110	3.00	3.00	3.00	3.00	3.00	2.00	5.00
111	2.00	2.00	2.00	2.00	3.00	3.00	3.00
112	3.00	3.00	3.00	3.00	5.00	3.00	5.00
113	3.00	3.00	3.00	3.00	5.00	2.00	5.00
114	3.00	3.00	3.00	5.00	5.00	3.00	4.00
115	5.00	3.00	2.00	5.00	4.00	4.00	4.00
116	2.00	2.00	2.00	2.00	3.00	3.00	3.00
117	2.00	2.00	2.00	2.00	3.00	3.00	3.00
118	3.00	3.00	2.00	5.00	5.00	4.00	4.00
119	5.00	3.00	2.00	5.00	4.00	4.00	4.00
120	3.00	3.00	2.00	5.00	4.00	2.00	4.00
121	4.00	3.00	4.00	5.00	4.00	4.00	4.00
122	2.00	2.00	2.00	2.00	2.00	2.00	2.00
123	5.00	3.00	2.00	5.00	4.00	4.00	4.00
124	2.00	2.00	2.00	2.00	3.00	3.00	3.00
125	2.00	2.00	2.00	2.00	2.00	2.00	2.00
126	2.00	2.00	2.00	2.00	3.00	2.00	3.00
127	2.00	2.00	2.00	2.00	3.00	3.00	3.00
128	2.00	2.00	2.00	5.00	5.00	3.00	5.00
129	2.00	2.00	2.00	2.00	5.00	3.00	5.00
130	5.00	3.00	2.00	5.00	4.00	4.00	4.00
131	3.00	2.00	2.00	2.00	3.00	3.00	3.00
132	2.00	2.00	2.00	2.00	2.00	2.00	2.00
133	5.00	3.00	2.00	5.00	4.00	4.00	4.00
134	3.00	3.00	3.00	3.00	3.00	3.00	5.00
135	2.00	2.00	2.00	2.00	5.00	3.00	5.00
136	2.00	2.00	2.00	2.00	5.00	3.00	5.00
137	3.00	3.00	2.00	5.00	4.00	4.00	4.00
138	3.00	3.00	2.00	5.00	4.00	4.00	4.00
139	2.00	2.00	2.00	2.00	5.00	3.00	5.00
140	5.00	3.00	2.00	5.00	4.00	4.00	4.00
141	3.00	3.00	3.00	3.00	3.00	3.00	5.00

	البريد	الديدان	التقنية	الحمايةت	تكلفةلتو	تكلفةستخ	مصدر
101	.	.	4.00	5.00	3.00	3.00	5.00
102	.	.	4.00	5.00	3.00	3.00	5.00
103	.	.	2.00	5.00	3.00	3.00	5.00
104	.	.	3.00	3.00	4.00	4.00	2.00
105	5.00	5.00	.	.	.	.	.
106	4.00	5.00	.	.	.	.	.
107	4.00	5.00	.	.	.	.	.
108	5.00	5.00	.	.	.	.	.
109	5.00	5.00	.	.	.	.	.
110	5.00	5.00	.	.	.	.	.
111	3.00	3.00	.	.	.	.	.
112	5.00	5.00	.	.	.	.	.
113	5.00	5.00	.	.	.	.	.
114	5.00	5.00	.	.	.	.	.
115	3.00	5.00	.	.	.	.	.
116	3.00	3.00	.	.	.	.	.
117	3.00	3.00	.	.	.	.	.
118	3.00	5.00	.	.	.	.	.
119	3.00	5.00	.	.	.	.	.
120	3.00	5.00	.	.	.	.	.
121	3.00	5.00	.	.	.	.	.
122	3.00	3.00	.	.	.	.	.
123	3.00	5.00	.	.	.	.	.
124	3.00	3.00	.	.	.	.	.
125	3.00	3.00	.	.	.	.	.
126	3.00	3.00	.	.	.	.	.
127	3.00	3.00	.	.	.	.	.
128	4.00	5.00	.	.	.	.	.
129	5.00	4.00	.	.	.	.	.
130	3.00	5.00	.	.	.	.	.
131	3.00	3.00	.	.	.	.	.
132	3.00	3.00	.	.	.	.	.
133	3.00	5.00	.	.	.	.	.
134	5.00	5.00	.	.	.	.	.
135	5.00	4.00	.	.	.	.	.
136	5.00	4.00	.	.	.	.	.
137	3.00	5.00	.	.	.	.	.
138	3.00	5.00	.	.	.	.	.
139	5.00	4.00	.	.	.	.	.
140	3.00	5.00	.	.	.	.	.
141	5.00	5.00	.	.	.	.	.

	var00001	ip	حمايةتتع	ضبط	دليل	الديبي	الد
101	5.00	7.00	6.00	3.00	5.00	2.00	4.00
102	5.00	8.00	6.00	3.00	5.00	4.00	2.00
103	5.00	7.00	6.00	2.00	3.00	4.00	4.00
104	2.00	7.00	6.00	1.00	5.00	4.00	2.00
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	var00005	البلاغ	كفاءة	الخوف	الرغبة	اكتشاف	محدودية
101	4.00	4.00	1.00	5.00	5.00	5.00	5.00
102	4.00	4.00	1.00	5.00	5.00	5.00	5.00
103	4.00	4.00	1.00	5.00	5.00	5.00	5.00
104	4.00	5.00	3.00	4.00	4.00	2.00	3.00
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	التشفير	سجل	auditing	مراقبة	الشبكة	report	مراجعة
101	5.00	5.00	5.00	5.00	5.00	5.00	5.00
102	5.00	5.00	5.00	5.00	5.00	5.00	5.00
103	5.00	5.00	5.00	5.00	5.00	5.00	5.00
104	4.00	4.00	4.00	3.00	3.00	4.00	4.00
105	4.00	5.00	5.00	5.00	4.00	5.00	4.00
106	4.00	5.00	4.00	4.00	5.00	5.00	3.00
107	4.00	5.00	4.00	4.00	5.00	5.00	3.00
108	3.00	4.00	5.00	3.00	4.00	5.00	4.00
109	3.00	5.00	5.00	5.00	4.00	5.00	4.00
110	3.00	5.00	5.00	5.00	4.00	5.00	4.00
111	4.00	5.00	5.00	3.00	4.00	4.00	4.00
112	4.00	5.00	5.00	5.00	4.00	5.00	4.00
113	4.00	5.00	5.00	5.00	4.00	5.00	4.00
114	4.00	5.00	4.00	4.00	4.00	5.00	3.00
115	4.00	5.00	4.00	4.00	5.00	5.00	3.00
116	4.00	5.00	5.00	3.00	4.00	4.00	4.00
117	4.00	5.00	5.00	3.00	4.00	4.00	4.00
118	4.00	5.00	4.00	4.00	4.00	5.00	3.00
119	4.00	5.00	4.00	4.00	5.00	5.00	3.00
120	4.00	5.00	4.00	4.00	5.00	5.00	3.00
121	4.00	5.00	4.00	4.00	5.00	5.00	3.00
122	2.00	5.00	4.00	4.00	3.00	5.00	4.00
123	4.00	5.00	4.00	4.00	5.00	5.00	3.00
124	5.00	5.00	5.00	5.00	4.00	5.00	5.00
125	2.00	5.00	4.00	4.00	3.00	5.00	4.00
126	3.00	5.00	5.00	5.00	4.00	5.00	5.00
127	4.00	5.00	5.00	3.00	4.00	4.00	4.00
128	5.00	5.00	5.00	5.00	4.00	5.00	5.00
129	5.00	5.00	5.00	5.00	4.00	5.00	5.00
130	4.00	5.00	4.00	4.00	5.00	5.00	3.00
131	5.00	5.00	5.00	5.00	4.00	4.00	4.00
132	2.00	5.00	4.00	4.00	3.00	5.00	4.00
133	4.00	5.00	4.00	4.00	5.00	5.00	3.00
134	4.00	5.00	5.00	5.00	4.00	5.00	4.00
135	5.00	5.00	5.00	5.00	4.00	5.00	5.00
136	5.00	5.00	5.00	5.00	4.00	5.00	5.00
137	4.00	5.00	4.00	4.00	5.00	5.00	3.00
138	4.00	5.00	4.00	4.00	5.00	5.00	3.00
139	5.00	5.00	5.00	5.00	4.00	5.00	5.00
140	4.00	5.00	4.00	4.00	5.00	5.00	3.00
141	4.00	5.00	5.00	5.00	4.00	5.00	4.00

	الجدران	تتبعمختر	تتبعمصدر	كسر	كشف	viewdisk	pkzip
101	5.00	5.00	5.00	4.00	5.00	5.00	3.00
102	5.00	5.00	5.00	4.00	5.00	5.00	3.00
103	5.00	5.00	5.00	4.00	5.00	5.00	3.00
104	4.00	3.00	4.00	4.00	4.00	4.00	4.00
105	5.00	3.00	3.00	3.00	5.00	5.00	4.00
106	4.00	5.00	5.00	5.00	5.00	3.00	3.00
107	4.00	5.00	5.00	5.00	5.00	3.00	3.00
108	5.00	3.00	3.00	3.00	5.00	5.00	1.00
109	5.00	3.00	3.00	3.00	5.00	5.00	1.00
110	5.00	4.00	4.00	3.00	5.00	5.00	1.00
111	4.00	4.00	4.00	3.00	5.00	3.00	3.00
112	5.00	3.00	3.00	3.00	5.00	5.00	1.00
113	5.00	4.00	2.00	3.00	5.00	5.00	1.00
114	4.00	5.00	5.00	5.00	4.00	3.00	3.00
115	4.00	5.00	5.00	5.00	5.00	3.00	3.00
116	4.00	4.00	4.00	3.00	5.00	3.00	3.00
117	4.00	4.00	4.00	3.00	5.00	3.00	3.00
118	4.00	5.00	5.00	5.00	5.00	3.00	3.00
119	4.00	5.00	5.00	5.00	5.00	3.00	3.00
120	4.00	5.00	5.00	5.00	5.00	3.00	3.00
121	4.00	5.00	5.00	5.00	4.00	3.00	3.00
122	4.00	4.00	4.00	3.00	5.00	3.00	2.00
123	4.00	5.00	5.00	5.00	5.00	3.00	3.00
124	5.00	2.00	4.00	5.00	5.00	3.00	3.00
125	4.00	4.00	4.00	3.00	5.00	3.00	2.00
126	5.00	4.00	4.00	5.00	5.00	3.00	3.00
127	4.00	4.00	4.00	3.00	5.00	3.00	3.00
128	5.00	4.00	4.00	5.00	4.00	3.00	3.00
129	5.00	4.00	4.00	5.00	4.00	3.00	3.00
130	4.00	5.00	5.00	5.00	5.00	3.00	3.00
131	4.00	4.00	4.00	3.00	4.00	3.00	3.00
132	4.00	4.00	4.00	3.00	4.00	3.00	2.00
133	4.00	5.00	5.00	5.00	5.00	3.00	3.00
134	5.00	3.00	3.00	3.00	5.00	5.00	4.00
135	5.00	4.00	4.00	5.00	4.00	3.00	3.00
136	5.00	4.00	4.00	5.00	4.00	3.00	3.00
137	4.00	5.00	5.00	5.00	5.00	3.00	3.00
138	4.00	5.00	5.00	5.00	5.00	3.00	3.00
139	5.00	4.00	4.00	5.00	4.00	3.00	3.00
140	4.00	5.00	5.00	5.00	5.00	3.00	3.00
141	5.00	3.00	3.00	3.00	5.00	5.00	4.00

	xtreepro	lantast	diskette	laplink	المقارنة	logging	تشريعات
101	4.00	4.00	3.00	3.00	5.00	5.00	5.00
102	4.00	4.00	3.00	3.00	5.00	5.00	5.00
103	4.00	4.00	3.00	3.00	5.00	5.00	5.00
104	4.00	4.00	3.00	3.00	5.00	4.00	4.00
105	3.00	2.00	3.00	3.00	4.00	5.00	5.00
106	3.00	3.00	4.00	4.00	4.00	5.00	5.00
107	3.00	3.00	4.00	4.00	4.00	5.00	5.00
108	2.00	2.00	3.00	3.00	2.00	5.00	5.00
109	3.00	2.00	3.00	3.00	4.00	5.00	5.00
110	3.00	2.00	4.00	3.00	2.00	5.00	5.00
111	4.00	2.00	3.00	4.00	3.00	5.00	4.00
112	3.00	2.00	3.00	3.00	2.00	5.00	5.00
113	3.00	2.00	3.00	3.00	4.00	5.00	5.00
114	3.00	1.00	4.00	4.00	4.00	4.00	5.00
115	3.00	3.00	4.00	3.00	4.00	4.00	5.00
116	4.00	2.00	3.00	4.00	3.00	5.00	4.00
117	4.00	2.00	3.00	4.00	3.00	5.00	4.00
118	3.00	3.00	4.00	4.00	4.00	4.00	5.00
119	3.00	3.00	4.00	3.00	4.00	4.00	5.00
120	3.00	3.00	4.00	4.00	4.00	5.00	5.00
121	3.00	3.00	4.00	4.00	4.00	5.00	5.00
122	2.00	3.00	3.00	3.00	3.00	5.00	3.00
123	3.00	3.00	4.00	3.00	4.00	4.00	5.00
124	2.00	2.00	3.00	2.00	3.00	5.00	4.00
125	4.00	3.00	3.00	3.00	3.00	4.00	3.00
126	4.00	2.00	3.00	4.00	3.00	5.00	4.00
127	4.00	2.00	3.00	4.00	3.00	5.00	4.00
128	4.00	2.00	3.00	4.00	3.00	5.00	4.00
129	3.00	2.00	3.00	2.00	2.00	5.00	4.00
130	3.00	3.00	4.00	3.00	4.00	4.00	5.00
131	4.00	2.00	3.00	2.00	3.00	5.00	4.00
132	4.00	3.00	3.00	3.00	3.00	4.00	3.00
133	3.00	3.00	4.00	3.00	4.00	4.00	5.00
134	2.00	3.00	3.00	3.00	4.00	5.00	5.00
135	3.00	2.00	3.00	2.00	2.00	5.00	4.00
136	3.00	2.00	3.00	2.00	2.00	5.00	4.00
137	2.00	2.00	4.00	3.00	4.00	4.00	5.00
138	2.00	2.00	4.00	3.00	4.00	4.00	5.00
139	3.00	2.00	3.00	2.00	2.00	5.00	4.00
140	3.00	3.00	4.00	3.00	4.00	4.00	5.00
141	2.00	3.00	3.00	3.00	4.00	5.00	5.00

	مكونات	متخصص	التحقيق	مستجدات	تحديث	قناعة	الشكوى
101	3.00	5.00	2.00	2.00	2.00	5.00	5.00
102	3.00	5.00	2.00	2.00	2.00	5.00	5.00
103	3.00	5.00	2.00	3.00	4.00	4.00	3.00
104	3.00	3.00	2.00	3.00	2.00	4.00	5.00
105	4.00	3.00	5.00	3.00	2.00	1.00	5.00
106	4.00	2.00	2.00	3.00	4.00	4.00	3.00
107	4.00	2.00	2.00	3.00	4.00	4.00	3.00
108	4.00	3.00	5.00	3.00	2.00	1.00	5.00
109	4.00	3.00	5.00	3.00	2.00	1.00	5.00
110	4.00	3.00	5.00	3.00	2.00	1.00	5.00
111	3.00	2.00	5.00	3.00	4.00	3.00	4.00
112	4.00	3.00	5.00	3.00	2.00	1.00	5.00
113	4.00	3.00	5.00	3.00	2.00	1.00	5.00
114	4.00	2.00	2.00	3.00	4.00	4.00	3.00
115	4.00	2.00	2.00	3.00	4.00	4.00	3.00
116	3.00	2.00	5.00	3.00	4.00	3.00	4.00
117	3.00	2.00	5.00	3.00	4.00	3.00	4.00
118	4.00	2.00	2.00	3.00	4.00	4.00	3.00
119	4.00	2.00	2.00	3.00	4.00	4.00	3.00
120	4.00	2.00	2.00	3.00	4.00	4.00	3.00
121	4.00	2.00	2.00	3.00	4.00	4.00	3.00
122	3.00	2.00	2.00	2.00	2.00	4.00	3.00
123	4.00	2.00	2.00	3.00	4.00	4.00	3.00
124	3.00	2.00	5.00	3.00	4.00	3.00	4.00
125	3.00	2.00	2.00	2.00	2.00	4.00	3.00
126	3.00	2.00	5.00	3.00	4.00	3.00	4.00
127	3.00	2.00	5.00	3.00	4.00	3.00	4.00
128	3.00	2.00	5.00	3.00	4.00	3.00	4.00
129	3.00	2.00	5.00	3.00	4.00	3.00	4.00
130	4.00	2.00	2.00	3.00	4.00	4.00	3.00
131	3.00	2.00	5.00	3.00	4.00	3.00	4.00
132	3.00	2.00	2.00	2.00	2.00	4.00	3.00
133	4.00	2.00	2.00	3.00	4.00	4.00	3.00
134	4.00	3.00	5.00	3.00	2.00	1.00	5.00
135	3.00	2.00	5.00	3.00	4.00	3.00	4.00
136	3.00	2.00	5.00	3.00	4.00	3.00	4.00
137	4.00	2.00	2.00	3.00	4.00	4.00	3.00
138	4.00	2.00	2.00	3.00	4.00	4.00	3.00
139	3.00	2.00	5.00	3.00	4.00	3.00	4.00
140	4.00	2.00	2.00	3.00	4.00	4.00	3.00
141	4.00	3.00	5.00	3.00	2.00	1.00	5.00

	يقاوم	تناسب	التدريب	الخبراء	تصميم	عنبعد	تنسيقاً
101	5.00	4.00	5.00	5.00	2.00	2.00	2.00
102	5.00	4.00	5.00	5.00	2.00	2.00	2.00
103	3.00	4.00	4.00	4.00	4.00	4.00	2.00
104	5.00	4.00	5.00	5.00	2.00	2.00	2.00
105	4.00	3.00	3.00	1.00	1.00	1.00	.
106	3.00	4.00	4.00	2.00	2.00	2.00	.
107	3.00	4.00	4.00	2.00	2.00	2.00	.
108	4.00	3.00	3.00	1.00	1.00	1.00	.
109	4.00	3.00	3.00	1.00	1.00	1.00	.
110	4.00	3.00	3.00	1.00	1.00	1.00	.
111	4.00	3.00	4.00	3.00	2.00	2.00	.
112	4.00	3.00	3.00	1.00	1.00	1.00	.
113	4.00	3.00	3.00	1.00	1.00	1.00	.
114	3.00	4.00	4.00	2.00	2.00	2.00	.
115	3.00	4.00	4.00	2.00	2.00	2.00	.
116	4.00	3.00	4.00	3.00	2.00	2.00	.
117	4.00	3.00	4.00	3.00	2.00	2.00	.
118	3.00	4.00	4.00	2.00	2.00	2.00	.
119	3.00	4.00	4.00	2.00	2.00	2.00	.
120	3.00	4.00	4.00	2.00	2.00	2.00	.
121	3.00	4.00	4.00	2.00	2.00	2.00	.
122	4.00	2.00	2.00	2.00	4.00	2.00	.
123	3.00	4.00	4.00	2.00	2.00	2.00	.
124	4.00	3.00	4.00	3.00	2.00	2.00	.
125	4.00	2.00	2.00	2.00	4.00	2.00	.
126	4.00	3.00	4.00	3.00	2.00	2.00	.
127	4.00	3.00	4.00	3.00	2.00	2.00	.
128	4.00	3.00	4.00	3.00	2.00	2.00	.
129	4.00	3.00	4.00	3.00	3.00	2.00	.
130	3.00	4.00	4.00	2.00	2.00	3.00	.
131	4.00	3.00	4.00	3.00	2.00	2.00	.
132	4.00	2.00	2.00	2.00	4.00	2.00	.
133	3.00	4.00	4.00	2.00	2.00	2.00	.
134	4.00	3.00	3.00	1.00	1.00	1.00	.
135	4.00	3.00	4.00	3.00	2.00	2.00	.
136	4.00	3.00	4.00	3.00	2.00	2.00	.
137	3.00	4.00	4.00	2.00	2.00	4.00	.
138	3.00	4.00	4.00	2.00	3.00	2.00	.
139	4.00	3.00	4.00	3.00	2.00	2.00	.
140	3.00	4.00	4.00	2.00	2.00	2.00	.
141	4.00	3.00	3.00	1.00	1.00	1.00	.

	تنسيقنم	مناسب	المختصين	معاهد	اهمية	التوعية	أشتراك
101	3.00	3.00	3.00	3.00	.	.	.
102	3.00	3.00	3.00	3.00	.	.	.
103	3.00	3.00	3.00	3.00	.	.	.
104	3.00	3.00	3.00	3.00	.	.	.
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	المهارة	المعرفة	المقدرة	بأساليب	الإثبات	الدوري	الزام
101	2.00	2.00	3.00	2.00	2.00	.	.
102	3.00	2.00	3.00	1.00	2.00	.	.
103	2.00	2.00	3.00	2.00	2.00	.	.
104	2.00	3.00	3.00	2.00	2.00	.	.
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	الحوافز	توزيع	التزكية	المصرح	بصمة	محركات	لصيانة
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	الأحتياط	تحديثها	المدة	المزامنة	تلائم	باستمرار	التقدم
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	تشكيل	رصد	التتبع	ربط	ضوابطتشغ	ضوابطعمل	ظوابطقاع
101	.	.	.	.	.	.	.
102	.	.	.	.	.	.	.
103	.	.	.	.	.	.	.
104	.	.	.	.	.	.	.
105	.	.	.	.	.	.	.
106	.	.	.	.	.	.	.
107	.	.	.	.	.	.	.
108	.	.	.	.	.	.	.
109	.	.	.	.	.	.	.
110	.	.	.	.	.	.	.
111	.	.	.	.	.	.	.
112	.	.	.	.	.	.	.
113	.	.	.	.	.	.	.
114	.	.	.	.	.	.	.
115	.	.	.	.	.	.	.
116	.	.	.	.	.	.	.
117	.	.	.	.	.	.	.
118	.	.	.	.	.	.	.
119	.	.	.	.	.	.	.
120	.	.	.	.	.	.	.
121	.	.	.	.	.	.	.
122	.	.	.	.	.	.	.
123	.	.	.	.	.	.	.
124	.	.	.	.	.	.	.
125	.	.	.	.	.	.	.
126	.	.	.	.	.	.	.
127	.	.	.	.	.	.	.
128	.	.	.	.	.	.	.
129	.	.	.	.	.	.	.
130	.	.	.	.	.	.	.
131	.	.	.	.	.	.	.
132	.	.	.	.	.	.	.
133	.	.	.	.	.	.	.
134	.	.	.	.	.	.	.
135	.	.	.	.	.	.	.
136	.	.	.	.	.	.	.
137	.	.	.	.	.	.	.
138	.	.	.	.	.	.	.
139	.	.	.	.	.	.	.
140	.	.	.	.	.	.	.
141	.	.	.	.	.	.	.

	ظوابطشبك	ضوابطالد	البشري	المكاني	المطورة	الجاهزة	الانترنت
101	.	.	5.00	5.00	4.00	4.00	5.00
102	.	.	5.00	5.00	5.00	4.00	5.00
103	.	.	3.00	5.00	5.00	4.00	2.00
104	.	.	4.00	5.00	4.00	3.00	5.00
105	.	.	4.00	5.00	4.00	5.00	4.00
106	.	.	4.00	5.00	3.00	5.00	3.00
107	.	.	4.00	5.00	3.00	5.00	5.00
108	.	.	4.00	5.00	4.00	5.00	4.00
109	.	.	4.00	5.00	4.00	5.00	4.00
110	.	.	4.00	5.00	4.00	5.00	4.00
111	.	.	5.00	5.00	4.00	3.00	4.00
112	.	.	4.00	5.00	4.00	4.00	4.00
113	.	.	4.00	5.00	4.00	4.00	4.00
114	.	.	4.00	5.00	3.00	5.00	5.00
115	.	.	4.00	5.00	3.00	5.00	5.00
116	.	.	5.00	5.00	4.00	3.00	4.00
117	.	.	5.00	5.00	4.00	3.00	4.00
118	.	.	4.00	5.00	3.00	5.00	5.00
119	.	.	4.00	5.00	2.00	1.00	5.00
120	.	.	4.00	5.00	3.00	5.00	5.00
121	.	.	4.00	5.00	2.00	5.00	5.00
122	.	.	5.00	5.00	4.00	4.00	4.00
123	.	.	4.00	5.00	3.00	5.00	5.00
124	.	.	5.00	5.00	5.00	4.00	5.00
125	.	.	5.00	5.00	4.00	5.00	4.00
126	.	.	5.00	5.00	5.00	5.00	5.00
127	.	.	5.00	5.00	4.00	3.00	4.00
128	.	.	5.00	5.00	5.00	5.00	5.00
129	.	.	5.00	5.00	5.00	5.00	5.00
130	.	.	4.00	5.00	3.00	5.00	5.00
131	.	.	5.00	5.00	4.00	5.00	4.00
132	.	.	5.00	5.00	4.00	5.00	4.00
133	.	.	4.00	5.00	3.00	5.00	5.00
134	.	.	4.00	5.00	4.00	5.00	4.00
135	.	.	5.00	5.00	5.00	5.00	5.00
136	.	.	5.00	5.00	5.00	5.00	5.00
137	.	.	4.00	5.00	3.00	5.00	5.00
138	.	.	4.00	5.00	3.00	5.00	5.00
139	.	.	5.00	5.00	5.00	5.00	5.00
140	.	.	4.00	5.00	3.00	5.00	5.00
141	.	.	4.00	5.00	4.00	5.00	4.00

	الخدمات	احترازات	وسائط	منافسين	السياسة	التشريعا	المجرمين
101	4.00	4.00	3.00	4.00	5.00	5.00	5.00
102	4.00	4.00	3.00	4.00	5.00	5.00	5.00
103	2.00	3.00	3.00	4.00	5.00	5.00	5.00
104	4.00	4.00	4.00	4.00	5.00	5.00	5.00
105	3.00	3.00	3.00	1.00	5.00	5.00	.
106	4.00	4.00	4.00	3.00	5.00	5.00	5.00
107	4.00	4.00	4.00	3.00	5.00	5.00	5.00
108	3.00	3.00	3.00	1.00	4.00	5.00	5.00
109	3.00	3.00	3.00	1.00	5.00	5.00	5.00
110	3.00	3.00	3.00	1.00	5.00	5.00	5.00
111	5.00	5.00	5.00	5.00	5.00	5.00	5.00
112	3.00	3.00	3.00	1.00	5.00	5.00	5.00
113	3.00	3.00	3.00	1.00	5.00	5.00	5.00
114	3.00	3.00	4.00	3.00	5.00	5.00	5.00
115	3.00	3.00	4.00	3.00	5.00	5.00	5.00
116	3.00	3.00	5.00	5.00	5.00	5.00	4.00
117	3.00	3.00	5.00	5.00	5.00	5.00	5.00
118	3.00	3.00	4.00	3.00	5.00	5.00	5.00
119	3.00	3.00	4.00	3.00	4.00	5.00	4.00
120	3.00	3.00	4.00	3.00	3.00	5.00	5.00
121	3.00	3.00	4.00	3.00	5.00	5.00	5.00
122	5.00	5.00	5.00	3.00	5.00	4.00	4.00
123	4.00	4.00	4.00	3.00	3.00	5.00	5.00
124	5.00	5.00	5.00	5.00	5.00	5.00	5.00
125	5.00	5.00	5.00	3.00	5.00	4.00	4.00
126	5.00	5.00	5.00	5.00	5.00	5.00	5.00
127	5.00	5.00	5.00	5.00	5.00	5.00	5.00
128	5.00	5.00	5.00	5.00	5.00	5.00	5.00
129	3.00	3.00	5.00	5.00	5.00	5.00	5.00
130	3.00	3.00	4.00	3.00	5.00	5.00	4.00
131	3.00	3.00	5.00	5.00	5.00	5.00	5.00
132	3.00	3.00	5.00	3.00	5.00	4.00	4.00
133	3.00	3.00	4.00	3.00	5.00	5.00	5.00
134	3.00	3.00	3.00	1.00	5.00	5.00	5.00
135	3.00	3.00	5.00	5.00	5.00	5.00	5.00
136	5.00	5.00	5.00	5.00	5.00	5.00	5.00
137	4.00	4.00	4.00	3.00	5.00	5.00	5.00
138	4.00	4.00	4.00	3.00	5.00	5.00	5.00
139	5.00	5.00	5.00	5.00	5.00	5.00	5.00
140	4.00	4.00	4.00	3.00	5.00	5.00	5.00
141	3.00	3.00	3.00	1.00	5.00	5.00	5.00

	الرؤساء	عقوبات	أعلان	lev_1	العينةz	zsc001	المطورةz
101	5.00	5.00	5.00	.24	.26253	.26253	-.05569
102	5.00	5.00	3.00	.24	.26253	.26253	1.25299
103	2.00	5.00	5.00	.24	.26253	.26253	1.25299
104	5.00	5.00	3.00	.24	.26253	.26253	-.05569
105	4.00	5.00	5.00	.05	1.45664	1.45664	-.05569
106	4.00	4.00	5.00	.09	1.45664	1.45664	-1.36437
107	4.00	5.00	5.00	.09	1.45664	1.45664	-1.36437
108	3.00	5.00	4.00	.31	1.45664	1.45664	-.05569
109	4.00	3.00	5.00	.41	1.45664	1.45664	-.05569
110	4.00	5.00	4.00	.36	1.45664	1.45664	-.05569
111	5.00	5.00	5.00	.17	1.45664	1.45664	-.05569
112	4.00	5.00	5.00	.42	1.45664	1.45664	-.05569
113	4.00	5.00	5.00	.12	1.45664	1.45664	-.05569
114	4.00	5.00	5.00	.19	1.45664	1.45664	-1.36437
115	4.00	5.00	5.00	.09	1.45664	1.45664	-1.36437
116	5.00	5.00	5.00	.17	1.45664	1.45664	-.05569
117	5.00	5.00	5.00	.17	1.45664	1.45664	-.05569
118	4.00	5.00	5.00	.12	1.45664	1.45664	-1.36437
119	4.00	5.00	5.00	.09	1.45664	1.45664	-2.67305
120	4.00	5.00	5.00	.10	1.45664	1.45664	-1.36437
121	4.00	5.00	5.00	.08	1.45664	1.45664	-2.67305
122	5.00	4.00	5.00	.29	1.45664	1.45664	-.05569
123	4.00	5.00	5.00	.09	1.45664	1.45664	-1.36437
124	5.00	5.00	5.00	.21	1.45664	1.45664	1.25299
125	5.00	4.00	5.00	.19	1.45664	1.45664	-.05569
126	5.00	5.00	5.00	.31	1.45664	1.45664	1.25299
127	5.00	5.00	5.00	.17	1.45664	1.45664	-.05569
128	5.00	5.00	5.00	.22	1.45664	1.45664	1.25299
129	5.00	5.00	5.00	.13	1.45664	1.45664	1.25299
130	4.00	5.00	5.00	.09	1.45664	1.45664	-1.36437
131	5.00	5.00	5.00	.14	1.45664	1.45664	-.05569
132	5.00	4.00	5.00	.13	1.45664	1.45664	-.05569
133	4.00	5.00	5.00	.09	1.45664	1.45664	-1.36437
134	4.00	5.00	5.00	.09	1.45664	1.45664	-.05569
135	5.00	5.00	5.00	.13	1.45664	1.45664	1.25299
136	5.00	5.00	5.00	.13	1.45664	1.45664	1.25299
137	4.00	5.00	5.00	.06	1.45664	1.45664	-1.36437
138	4.00	5.00	5.00	.07	1.45664	1.45664	-1.36437
139	5.00	5.00	5.00	.13	1.45664	1.45664	1.25299
140	4.00	5.00	5.00	.09	1.45664	1.45664	-1.36437
141	4.00	5.00	5.00	.09	1.45664	1.45664	-.05569

	الجاهزةz	الانترنz	الخدماتz	احترازاz	وسائطz	منافسينz
101	-.63907	.83704	.17560	.24176	-1.25299	.50973
102	-.63907	.83704	.17560	.24176	-1.25299	.50973
103	-.63907	-4.22109	-2.43071	-1.02077	-1.25299	.50973
104	-2.00437	.83704	.17560	.24176	.05569	.50973
105	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
106	.72622	-2.53504	.17560	.24176	.05569	-.17476
107	.72622	.83704	.17560	.24176	.05569	-.17476
108	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
109	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
110	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
111	-2.00437	-.84900	1.47876	1.50430	1.36437	1.19422
112	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
113	-.63907	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
114	.72622	.83704	-1.12755	-1.02077	.05569	-.17476
115	.72622	.83704	-1.12755	-1.02077	.05569	-.17476
116	-2.00437	-.84900	-1.12755	-1.02077	1.36437	1.19422
117	-2.00437	-.84900	-1.12755	-1.02077	1.36437	1.19422
118	.72622	.83704	-1.12755	-1.02077	.05569	-.17476
119	-4.73495	.83704	-1.12755	-1.02077	.05569	-.17476
120	.72622	.83704	-1.12755	-1.02077	.05569	-.17476
121	.72622	.83704	-1.12755	-1.02077	.05569	-.17476
122	-.63907	-.84900	1.47876	1.50430	1.36437	-.17476
123	.72622	.83704	.17560	.24176	.05569	-.17476
124	-.63907	.83704	1.47876	1.50430	1.36437	1.19422
125	.72622	-.84900	1.47876	1.50430	1.36437	-.17476
126	.72622	.83704	1.47876	1.50430	1.36437	1.19422
127	-2.00437	-.84900	1.47876	1.50430	1.36437	1.19422
128	.72622	.83704	1.47876	1.50430	1.36437	1.19422
129	.72622	.83704	-1.12755	-1.02077	1.36437	1.19422
130	.72622	.83704	-1.12755	-1.02077	.05569	-.17476
131	.72622	-.84900	-1.12755	-1.02077	1.36437	1.19422
132	.72622	-.84900	-1.12755	-1.02077	1.36437	-.17476
133	.72622	.83704	-1.12755	-1.02077	.05569	-.17476
134	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374
135	.72622	.83704	-1.12755	-1.02077	1.36437	1.19422
136	.72622	.83704	1.47876	1.50430	1.36437	1.19422
137	.72622	.83704	.17560	.24176	.05569	-.17476
138	.72622	.83704	.17560	.24176	.05569	-.17476
139	.72622	.83704	1.47876	1.50430	1.36437	1.19422
140	.72622	.83704	.17560	.24176	.05569	-.17476
141	.72622	-.84900	-1.12755	-1.02077	-1.25299	-1.54374

ملحق (ب) يبين خصائص عينة الدراسة

جدول رقم (1) يوضح نوع عينة الدراسة

نوع العينة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
العاملين	68	48.2	48.2	48.2
المحققين	36	25.5	25.5	73.8
الموفرين	37	26.2	26.2	100.0
المجموع	141	100.0	100.0	

جدول رقم (2) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً للتخصص

التخصص	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أداري	14	9.9	20.6	20.6
محلل نظم	7	5.0	10.3	30.9
مبرمج	11	7.8	16.2	47.1
مدير قاعدة بيانات	2	1.4	2.9	50.0
مدير نظام	4	2.8	5.9	55.9
مدقق	8	5.7	11.8	67.6
مدير موقع	3	2.1	4.4	72.1
أخصائي أمن معلومات	15	10.6	22.1	94.1
مهندس شبكات	4	2.8	5.9	100.0
المجموع	68	48.2	100.0	

جدول رقم (3) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لنوع المؤسسة التي ينتمون لها

نوع المؤسسة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
قطاع حكومي	11	7.8	16.2	16.2
قطاع مصرفي	11	7.8	16.2	32.4
شركة متخصصة في مجال تقنية المعلومات	34	24.1	50.0	82.4
شركة غير متخصصة في مجال تقنية المعلومات	12	8.5	17.6	100.0
المجموع	68	48.2	100.0	

جدول رقم (4) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لعدد أجهزة الحاسب الآلي في مؤسستهم

عدد أجهزة الحاسب الآلي في المنظمة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أقل من 100	20	14.2	29.4	29.4
من 100 إلى 1000	17	12.1	25.0	54.4
أكثر من 1000	31	22.0	45.6	100.0
المجموع	68	48.2	100.0	

جدول رقم (5) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لنسبة المصروفات على تقنية المعلومات إلى أجمالي الميزانية

نسبة المصروفات على تقنية المعلومات	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أقل من 10 بالمائة	14	9.9	20.6	20.6
من 10بالمائة إلى أقل من 30 بالمائة	12	8.5	17.6	38.2
من 30 بالمائة إلى 50 بالمائة	29	20.6	42.6	80.9
أكثر من 50بالمائة	13	9.2	19.1	100.0
المجموع	68	48.2	100.0	

جدول رقم (6) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لتوفر خدمة الإنترنت للموظفين

مدى توفر خدمة الإنترنت	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
تتوفر للجميع	34	24.1	50.0	50.0
تتوفر للبعض	33	23.4	48.5	98.5
لا تتوفر	1	.7	1.5	100.0
المجموع	68	48.2	100.0	

جدول رقم (7) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لأسلوب الدخول للإنترنت

أسلوب الدخول للإنترنت	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
الخطوط الهاتفية	5	3.5	7.4	7.4
الشبكة المحلية المربوطة بمزود الخدمة	59	41.8	86.8	94.1
شبكة مستقلة عن شبكة العمل	3	2.1	4.4	98.5
لا يوجد أطلاقاً	1	.7	1.5	100.0
المجموع	68	48.2	100.0	

جدول رقم (8) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لوجود سياسة أمنية لتعامل مع الحاسب الآلي والإنترنت

مدى وجود سياسة أمنية	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نعم	54	38.3	79.4	79.4
لا	14	9.9	20.6	100.0
المجموع	68	48.2	100.0	

جدول رقم (9) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لوجود قسم متخصص في أمن المعلومات

وجود قسم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نعم	50	35.5	73.5	73.5
لا	18	12.8	26.5	100.0
المجموع	68	48.2	100.0	

جدول رقم (10) يوضح توزيع عينة الدراسة (العاملين بالنظم) وفقاً لعدد العاملين في قسم الأمن

عدد العاملين	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
1	2	1.4	4.0	4.0
من 2 إلى 5	9	6.4	18.0	22.0
من 6 إلى 10	15	10.6	30.0	52.0
من 11 إلى 20	12	8.5	24.0	76.0
من 21 إلى 50	12	8.5	24.0	100.0
المجموع	50	35.5	100.0	

ملحق (جـ) يبين نتائج الدراسة

جدول رقم (1) يوضح استجابة (المحققين، والعاملين بالنظم، والموفرين) نحو العناصر المتعلقة بمكونات السياسة الأمنية مرتبة حسب أهميتها لدى العينة

نوع العنصر	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
وجود سياسة أمنية خاصة لأمن نظم المعلومات في المنظمة التي تعمل بها	4.96	5.00	5.00	.2638	2.00	699.00
الزام الموظفين بالسياسة الأمنية ووضع عقوبات للمخالفين	4.93	5.00	5.00	.2840	2.00	695.00
وجود سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية	4.91	5.00	5.00	.2913	1.00	687.00
يتم أعلان السياسة الامنية للموظفين بما يكفل تبليغها للعموم	4.81	5.00	5.00	.5334	3.00	678.00
تقيد الرؤساء بالسياسة الأمنية عند أعطاء التعليمات	4.42	4.00	4.00	.5874	3.00	623.00

جدول (1- أ) يوضح استجابتهم نحو وجود سياسة أمنية خاصة لأمن نظم المعلومات في المنظمة التي تعمل بها

مدى الموافقة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
موافق إلى حدٍ ما	2	1.4	1.4	1.4
موافق	2	1.4	1.4	2.8
موافق بشدة	137	97.2	97.2	100.0
المجموع	141	100.0	100.0	

جدول (1- ب) يوضح استجابتهم لمدى اللزام الموظفين بالسياسة الأمنية ووضع عقوبات للمخالفين

مدى الموافقة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
موافق إلى حدٍ ما	1	.7	.7	.7
موافق	8	5.7	5.7	6.4
موافق بشدة	132	93.6	93.6	100.0
المجموع	141	100.0	100.0	

جدول (1- جـ) يوضح استجابتهم لمدى وجود سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية

مدى الموافقة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
موافق	13	9.2	9.3	9.3
موافق بشدة	127	90.1	90.7	100.0
المجموع	140	99.3	100.0	
لم يستجيبوا	1	.7		

جدول (1- د) يوضح استجابتهم لمدى أعلان السياسة الامنية للموظفين بما يكفل تبليغها للعموم

مدى الموافقة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق	2	1.4	1.4	1.4
موافق إلى حدٍ ما	3	2.1	2.1	3.5
موافق	15	10.6	10.6	14.2
موافق بشدة	121	85.8	85.8	100.0
المجموع	141	100.0	100.0	

جدول (1- هـ) يوضح استجابتهم لمدى تقيد الرؤساء بالسياسة الأمنية عند أعطاء التعليمات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق	1	.7	.7	.7
موافق إلى حدٍ ما	4	2.8	2.8	3.5
موافق	71	50.4	50.4	53.9
موافق بشدة	65	46.1	46.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (2) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح الجانب البشري من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
ليس موجود وضرورياً	9	6.4	6.4	6.4
موجود وغير واضح	71	50.4	50.4	56.7
موجود وواضح	61	43.3	43.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (3) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح الموقع المكاني لخدمات التقنية المعلوماتية من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
ليس موجود وغير ضرورياً	1	.7	.7	.7
ليس موجود وضرورياً	5	3.5	3.5	4.3
موجود وغير واضح	21	14.9	14.9	19.1
موجود وواضح	114	80.9	80.9	100.0
المجموع	141	100.0	100.0	

جدول رقم (4) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح البرامج المطورة داخلياً من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
ليس موجود وغير ضرورياً	3	2.1	2.1	2.1
ليس موجود وضرورياً	29	20.6	20.6	22.7
موجود وغير واضح	68	48.2	48.2	70.9
موجود وواضح	41	29.1	29.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (5) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح البرامج الجاهزة من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا أدري	1	.7	.7	.7
ليس موجود وضرورياً	14	9.9	9.9	10.6
موجود وغير واضح	43	30.5	30.5	41.1
موجود وواضح	83	58.9	58.9	100.0
المجموع	141	100.0	100.0	

جدول رقم (6) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح استخدام الأنترنت من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
ليس موجود وغير ضرورياً	1	.7	.7	.7
ليس موجود وضرورياً	4	2.8	2.8	3.5
موجود وغير واضح	59	41.8	41.8	45.4
موجود وواضح	77	54.6	54.6	100.0
المجموع	141	100.0	100.0	

جدول رقم (7) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح التشارك في الخدمات من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
ليس موجود وغير ضرورياً	1	.7	.7	.7
ليس موجود وضرورياً	49	34.8	34.8	35.5
موجود وغير واضح	59	41.8	41.8	77.3
موجود وواضح	32	22.7	22.7	100.0
المجموع	141	100.0	100.0	

جدول رقم (8) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح الاحترازات الشخصية من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
ليس موجود وغير ضرورياً	1	.7	.7	.7
ليس موجود وضرورياً	57	40.4	40.4	41.1
موجود وغير واضح	51	36.2	36.2	77.3
موجود وواضح	32	22.7	22.7	100.0
المجموع	141	100.0	100.0	

جدول رقم (9) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح الوثائق ووسائط الحفظ من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
ليس موجود وضرورياً	44	31.2	31.2	31.2
موجود وغير واضح	59	41.8	41.8	73.0
موجود وواضح	38	27.0	27.0	100.0
المجموع	141	100.0	100.0	

جدول رقم (10) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، والموفرين) نحو وجود ووضوح العلاقة بين المنافسين والشركاء من ضمن مكونات السياسة الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا أدري	34	24.1	24.1	24.1
ليس موجود وضرورياً	37	26.2	26.2	50.4
موجود وغير واضح	36	25.5	25.5	75.9
موجود وواضح	34	24.1	24.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (11) يوضح مدى وعي عينة الدراسة العاملين بالنظم بأهمية أمن المعلومات

البيان	ما أهمية وجود إجراءات إدارية و فنية لأمن نظم المعلومات
المتوسط	4.9265
الوسيط	5.0000
المنوال	5.00
الانحراف المعياري	.3146
المدى	2.00
المجموع	335.00

جدول رقم (11- أ) يوضح استجابة العاملين بالنظم حيال أهمية وجود إجراءات إدارية و فنية لأمن نظم المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم إلى حدٍ ما	1	.7	1.5	1.5
مهم	3	2.1	4.4	5.9
مهم جداً	64	45.4	94.1	100.0
المجموع	68	48.2	100.0	

جدول رقم (12) يوضح استجابة العاملين بالنظم حيال كيفية التوعية في مجال أمن المعلومات للعاملين في المنظمة

العنصر	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا توجد	10	7.1	14.7	14.7
نشرات داخلية	23	16.3	33.8	48.5
ندوات ومحاضرات	11	7.8	16.2	64.7
نشرات ودوريات	22	15.6	32.4	97.1
نشرات ودوريات ومحاضرات	2	1.4	2.9	100.0
المجموع	68	48.2	100.0	

جدول رقم (13) يوضح استجابة عينة الدراسة (العاملين بالنظم) حول إتباع الأجراءاءت الأمنية مرتبة حسب مستوى إتباعها

الإجراء الأمني	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
اختيار نوعية مناسبة من وسائل الحماية تلائم نوع التطبيق	4.16	4.000	4.00	.7844	3.00	283
توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم	4.04	4.000	4.00	.2069	1.00	275
الضوابط الأمنية لبناء وتشغيل البرامج التطبيقية	3.96	4.000	4.00	.6092	3.00	269
عدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين	3.93	4.000	4.00	.3589	3.00	267
الزام العاملين بالنظم الإدارية المحددة	3.74	4.000	4.00	.6376	3.00	254
الطلب ممن يلتحق حديثا بالخدمة تزكية كشرط للتوظيف	3.74	4.000	4.00	.6376	3.00	254
الإجراءات التي تكفل أمن النسخ الاحتياطي ووسائط الحفظ الخارجية	3.71	3.000	3.00	.9314	2.00	252
الإجراءات الأمنية لصيانة الأجهزة	3.66	3.000	3.00	.8913	2.00	249
ضوابط عمليات الإدخال والإخراج	3.62	4.000	3.00	.6917	3.00	246
رصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم	3.50	4.000	4.00	1.1525	4.00	238
الضوابط المنظمة لعمليات التشغيل	3.38	3.000	3.00	.5738	2.00	230
تحديث برامج الحماية باستمرار	3.47	4.000	4.00	1.4086	4.00	236
استخدام وسائل حماية تساعد في تتبع المجرمين	3.37	3.000	3.00	1.1578	4.00	229
ضوابط إدارة الشبكات وخطوط الاتصال	3.31	3.000	3.00	.7382	3.00	225
استخدام التقنية للدخول على الأنظمة (بصمة (الإصبع، بصمة العين	3.32	4.000	4.00	1.5876	4.00	226
ضوابط مبرمجي قواعد البيانات ومدرائها	3.31	4.000	4.00	1.0112	3.00	225
إجراءات تحديث النسخ الاحتياطي المركزي	3.19	2.000	2.00	1.3850	3.00	217
تشكيل فريق طواري للتعامل مع الجريمة	3.07	3.000	4.00	1.1758	4.00	209
التقدم بشكوى حول جرائم نظم المعلومات	2.96	3.000	3.00	.7617	2.00	201
تحديد مدة صلاحية كلمات المرور وتغييرها	2.75	2.000	2.00	.9831	3.00	187
ربط الترقية والدورات (الحوافز الأخرى) بمدى التقيد بأمن المعلومات	2.66	3.000	1.00	1.2884	4.00	181
التأكد من مزامنة ساعات الأجهزة باستمرار	2.44	2.000	2.00	1.3088	4.00	166
منح الحوافز للإلتزام بالإجراءات الأمنية	2.25	2.000	2.00	1.1766	4.00	153
توفير إجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها	2.21	3.000	3.00	1.0729	3.00	150

جدول (13- أ) يوضح استجابتهم حيال اختيار نوعية مناسبة من وسائل الحماية تلائم نوع التطبيق

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	5	3.5	7.4	7.4
أحياناً	1	.7	1.5	8.8
غالباً	40	28.4	58.8	67.6
دائماً	22	15.6	32.4	100.0
المجموع	68	48.2	100.0	

جدول (13- ب) يوضح استجابتهم حيال توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غالباً	65	46.1	95.6	95.6
دائماً	3	2.1	4.4	100.0
المجموع	68	48.2	100.0	

جدول (13- جـ) يوضح استجابتهم حيال الضوابط الأمنية لبناء وتشغيل البرامج التطبيقية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	4	2.8	5.9	5.9
أحياناً	2	1.4	2.9	8.8
غالباً	55	39.0	80.9	89.7
دائماً	7	5.0	10.3	100.0
المجموع	68	48.2	100.0	

جدول (13- د) يوضح استجابتهم حيال عدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	1	.7	1.5	1.5
أحياناً	4	2.8	5.9	7.4
غالباً	62	44.0	91.2	98.5
دائماً	1	.7	1.5	100.0
المجموع	68	48.2	100.0	

جدول (13- هـ) يوضح استجابتهم حيال اللزام العاملين بالنظم الإدارية المحددة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	1	.7	1.5	1.5
أحياناً	22	15.6	32.4	33.8
غالباً	39	27.7	57.4	91.2
دائماً	6	4.3	8.8	100.0
المجموع	68	48.2	100.0	

جدول (13- و) يوضح استجابتهم حيال الطلب ممن يلتحق حديثاً بالخدمة تزكية كشرط للتوظيف

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	3	2.1	4.4	4.4
أحياناً	16	11.3	23.5	27.9
غالباً	45	31.9	66.2	94.1
دائماً	4	2.8	5.9	100.0
المجموع	68	48.2	100.0	

جدول (13- ز) يوضح استجابتهم حيال الإجراءات التي تكفل أمن النسخ الاحتياطي ووسائط الحفظ الخارجية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أحياناً	42	29.8	61.8	61.8
غالباً	4	2.8	5.9	67.6
دائماً	22	15.6	32.4	100.0
المجموع	68	48.2	100.0	

جدول (13- ح) يوضح استجابتهم حيال الإجراءات الأمنية لصيانة الأجهزة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أحياناً	42	29.8	61.8	61.8
غالباً	7	5.0	10.3	72.1
دائماً	19	13.5	27.9	100.0
المجموع	68	48.2	100.0	

جدول (13- ط) يوضح استجابتهم حيال ضوابط عمليات الإدخال والإخراج

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	1	.7	1.5	1.5
أحياناً	31	22.0	45.6	47.1
غالباً	29	20.6	42.6	89.7
دائماً	7	5.0	10.3	100.0
المجموع	68	48.2	100.0	

جدول (13- ي) يوضح استجابتهم حيال رصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	5	3.5	7.4	7.4
نادراً	8	5.7	11.8	19.1
أحياناً	16	11.3	23.5	42.6
غالباً	26	18.4	38.2	80.9
دائماً	13	9.2	19.1	100.0
المجموع	68	48.2	100.0	

جدول (13- ك) يوضح استجابتهم حيال الضوابط المنظمة لعمليات التشغيل

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	3	2.1	4.4	4.4
أحياناً	36	25.5	52.9	57.4
غالباً	29	20.6	42.6	100.0
المجموع	68	48.2	100.0	

جدول (13- ل) يوضح استجابتهم حيال تحديث برامج الحماية باستمرار

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	12	8.5	17.6	17.6
نادراً	6	4.3	8.8	26.5
أحياناً	4	2.8	5.9	32.4
غالباً	30	21.3	44.1	76.5
دائماً	16	11.3	23.5	100.0
المجموع	68	48.2	100.0	

جدول (13- م) يوضح استجابتهم حيال استخدام وسائل حماية تساعد في تتبع المجرمين

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	7	5.0	10.3	10.3
نادراً	4	2.8	5.9	16.2
أحياناً	26	18.4	38.2	54.4
غالباً	19	13.5	27.9	82.4
دائماً	12	8.5	17.6	100.0
المجموع	68	48.2	100.0	

جدول (13- س) يوضح استجابتهم حيال ضوابط إدارة الشبكات وخطوط الاتصال

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	2	1.4	2.9	2.9
نادراً	5	3.5	7.4	10.3
أحياناً	31	22.0	45.6	55.9
غالباً	30	21.3	44.1	100.0
المجموع	68	48.2	100.0	

(جدول (13- ع) يوضح استجابتهم حيال استخدام التقنية للدخول على الأنظمة (بصمة الإصبع، بصمة العين، البطاقات الممغنطة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	19	13.5	27.9	27.9
نادراً	2	1.4	2.9	30.9
أحياناً	3	2.1	4.4	35.3
غالباً	26	18.4	38.2	73.5
دائماً	18	12.8	26.5	100.0
المجموع	68	48.2	100.0	

جدول (13- ف) يوضح استجابتهم حيال ضوابط مبرمجي قواعد البيانات ومدرائها

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	9	6.4	13.2	13.2
أحياناً	20	14.2	29.4	42.6
غالباً	39	27.7	57.4	100.0
المجموع	68	48.2	100.0	

جدول (13- ص) يوضح استجابتهم حيال إجراءات تحديث النسخ الاحتياطي المركزي

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	37	26.2	54.4	54.4
أحياناً	3	2.1	4.4	58.8
غالباً	6	4.3	8.8	67.6
دائماً	22	15.6	32.4	100.0
المجموع	68	48.2	100.0	

جدول (13- ق) يوضح استجابتهم حيال تشكيل فريق طواري للتعامل مع الجريمة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	5	3.5	7.4	7.4
نادراً	23	16.3	33.8	41.2
أحياناً	8	5.7	11.8	52.9
غالباً	26	18.4	38.2	91.2
دائماً	6	4.3	8.8	100.0
المجموع	68	48.2	100.0	

جدول (13- ر) يوضح استجابتهم حيال التقدم بشكوى حول جرائم نظم المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	21	14.9	30.9	30.9
أحياناً	29	20.6	42.6	73.5
غالباً	18	12.8	26.5	100.0
المجموع	68	48.2	100.0	

جدول (13- ش) يوضح استجابتهم حيال تحديد مدة صلاحية كلمات المرور وتغييرها

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	2	1.4	2.9	2.9
نادراً	37	26.2	54.4	57.4
أحياناً	5	3.5	7.4	64.7
غالباً	24	17.0	35.3	100.0
المجموع	68	48.2	100.0	

جدول (13- ت) يوضح استجابتهم حيال ربط الترقية والدورات (الحوافز الأخرى) بمدى التقيد بأمن المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	18	12.8	26.5	26.5
نادراً	13	9.2	19.1	45.6
أحياناً	15	10.6	22.1	67.6
غالباً	18	12.8	26.5	94.1
دائماً	4	2.8	5.9	100.0
المجموع	68	48.2	100.0	

جدول (13- ث) يوضح استجابتهم حيال التأكد من مزامنة ساعات الأجهزة باستمرار

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	18	12.8	26.5	26.5
نادراً	24	17.0	35.3	61.8
أحياناً	13	9.2	19.1	80.9
غالباً	4	2.8	5.9	86.8
دائماً	9	6.4	13.2	100.0
المجموع	68	48.2	100.0	

جدول (13- خ) يوضح استجابتهم حيال منح الحوافز للإلتزام بالإجراءات الأمنية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	16	11.3	23.5	23.5
نادراً	35	24.8	51.5	75.0
أحياناً	9	6.4	13.2	88.2
دائماً	8	5.7	11.8	100.0
المجموع	68	48.2	100.0	

جدول (13- ذ) يوضح استجابتهم حيال توفير إجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يتبع أطلاقاً	29	20.6	42.6	42.6
أحياناً	35	24.8	51.5	94.1
غالباً	4	2.8	5.9	100.0
المجموع	68	48.2	100.0	

جدول رقم (14) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم) إزاء حجم حدوث جرائم نظم المعلومات مرتبة حسب حجم حدوثها

نمط الجريمة	المتوسط	الانحراف المعياري
إرسال وزراعة فيروسات	4.06	1.26
نسخ البرامج والاستخدام غير المصرح به	3.89	1.24
التلاعب بإدخال البيانات	3.88	1.12
تغيير البرامج والأعدادات	3.86	.89
إرسال احصنة طروادة	3.82	.76
الاستيلاء على ما سوى المعلومات	3.38	.88
تغيير البيانات بعد إدخالها	3.3269	1.2263
تدمير الملفات وقواعد البيانات	3.25	.81
الاختراقات البريد الاكتروني	3.24	1.07
نسخ البيانات لاستفادة منها	3.13	1.07
إعتراض الرسائل والتنصت على الشبكات	3.09	.62
التنصت والسرقة البيانات	2.99	.98
تعطيل المواقع والبرامج والأجهزة	2.87	1.13
إغراق البريد الإلكتروني	2.75	1.19

جدول رقم (14- أ) يوضح استجابتهم حيال إرسال وزراعة فيروسات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	10	7.1	9.6	9.6
محدود	4	2.8	3.8	13.5
متوسط	7	5.0	6.7	20.2
عالي	32	22.7	30.8	51.0
عالي جداً	51	36.2	49.0	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- ب) يوضح استجابتهم حيال حجم نسخ البرامج والاستخدام غير المصرح به

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	20	14.2	19.2	19.2
متوسط	25	17.7	24.0	43.3
عالي	5	3.5	4.8	48.1
عالي جداً	54	38.3	51.9	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- جـ) يوضح استجابتهم حيال حجم التلاعب بإدخال البيانات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	5	3.5	4.8	4.8
محدود	6	4.3	5.8	10.6
متوسط	24	17.0	23.1	33.7
عالي	31	22.0	29.8	63.5
عالي جداً	38	27.0	36.5	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- د) يوضح استجابتهم حيال حجم تغيير البرامج والأعدادات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	9	6.4	8.7	8.7
متوسط	22	15.6	21.2	29.8
عالي	48	34.0	46.2	76.0
عالي جداً	25	17.7	24.0	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- هـ) يوضح استجابتهم حيال حجم إرسال احصنة طروادة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	2	1.4	1.9	1.9
محدود	9	6.4	8.7	10.6
متوسط	2	1.4	1.9	12.5
عالي	84	59.6	80.8	93.3
عالي جداً	7	5.0	6.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- و) يوضح استجابتهم حيال حجم الاستيلاء على ما سوى المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	5	3.5	4.8	4.8
محدود	6	4.3	5.8	10.6
متوسط	44	31.2	42.3	52.9
عالي	42	29.8	40.4	93.3
عالي جداً	7	5.0	6.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- ز) يوضح استجابتهم حيال حجم تغيير البيانات بعد إدخالها

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	15	10.6	14.4	14.4
محدود	5	3.5	4.8	19.2
متوسط	31	22.0	29.8	49.0
عالي	37	26.2	35.6	84.6
عالي جداً	16	11.3	15.4	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- ح) يوضح استجابتهم حيال حجم تدمير الملفات وقواعد البيانات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	2	1.4	1.9	1.9
محدود	13	9.2	12.5	14.4
متوسط	51	36.2	49.0	63.5
عالي	33	23.4	31.7	95.2
عالي جداً	5	3.5	4.8	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- ط) يوضح استجابتهم حيال حجم الاختراقات البريد الاكتروني

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	13	9.2	12.5	12.5
محدود	7	5.0	6.7	19.2
متوسط	29	20.6	27.9	47.1
عالي	52	36.9	50.0	97.1
عالي جداً	3	2.1	2.9	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- ي) يوضح استجابتهم حيال حجم نسخ البيانات لاستفادة منها

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	15	10.6	14.4	14.4
محدود	8	5.7	7.7	22.1
متوسط	29	20.6	27.9	50.0
عالي	52	36.9	50.0	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- ك) يوضح استجابتهم حيال حجم إعتراض الرسائل والتنصت على الشبكات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	4	2.8	3.8	3.8
محدود	4	2.8	3.8	7.7
متوسط	75	53.2	72.1	79.8
عالي	21	14.9	20.2	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- ل) يوضح استجابتهم حيال حجم التنصت والسرقة البيانات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	15	10.6	14.4	14.4
محدود	5	3.5	4.8	19.2
متوسط	50	35.5	48.1	67.3
عالي	34	24.1	32.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- م) يوضح استجابتهم حيال حجم تعطيل المواقع والبرامج والأجهزة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	21	14.9	20.2	20.2
محدود	9	6.4	8.7	28.8
متوسط	39	27.7	37.5	66.3
عالي	33	23.4	31.7	98.1
عالي جداً	2	1.4	1.9	100.0
المجموع	104	73.8	100.0	

جدول رقم (14- د) يوضح استجابتهم حيال حجم إغراق البريد الإلكتروني

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يحدث	21	14.9	20.2	20.2
محدود	13	9.2	12.5	32.7
متوسط	54	38.3	51.9	84.6
عالي	3	2.1	2.9	87.5
عالي جداً	13	9.2	12.5	100.0
المجموع	104	73.8	100.0	

جدول رقم (15) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم) إزاء مدى حدوث جرائم نظم المعلومات بالمؤسسات

العنصر	العينة		المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
	العدد	لم يجب						
خطور جرائم نظم المعلومات	104	37	4.58	5.00	5	.78	4	476
معدل جرائم نظم المعلومات بعد ظهور الإنترنت	104	37	4.48	5.00	5	.84	2	466
حجم جرائم نظم المعلومات مقارنة بحجم الجرائم الاخرى في المنظمة	104	37	3.62	4.00	4	1.16	4	376
حجم الجرائم التي تم الإعلان عنها بالمنظمة	104	37	2.75	3.00	2	.98	3	286

جدول رقم (15- أ) يوضح استجابتهم حيال حجم خطور جرائم نظم المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	1	.7	1.0	1.0
محدود	2	1.4	1.9	2.9
متوسط	7	5.0	6.7	9.6
عالي	20	14.2	19.2	28.8
عالي جداً	74	52.5	71.2	100.0
المجموع	104	73.8	100.0	

جدول رقم (15- ب) يوضح استجابتهم حيال معدل جرائم نظم المعلومات بعد ظهور الإنترنت

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوسط	23	16.3	22.1	22.1
عالي	8	5.7	7.7	29.8
عالي جداً	73	51.8	70.2	100.0
المجموع	104	73.8	100.0	

جدول رقم (15- جـ) يوضح استجابتهم حيال معدل حجم جرائم نظم المعلومات مقارنة بحجم الجرائم الاخرى في المؤسسة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	1	.7	1.0	1.0
محدود	30	21.3	28.8	29.8
متوسط	1	.7	1.0	30.8
عالي	48	34.0	46.2	76.9
عالي جداً	24	17.0	23.1	100.0
المجموع	104	73.8	100.0	

جدول رقم (15- د) يوضح استجابتهم حيال حجم الجرائم التي تم الإعلان عنها بالمؤسسة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	10	7.1	9.6	9.6
محدود	36	25.5	34.6	44.2
متوسط	28	19.9	26.9	71.2
عالي	30	21.3	28.8	100.0
المجموع	104	73.8	100.0	

جدول رقم (16) يوضح استجابة عينة الدراسة (العاملين بالنظم) إزاء عدد مرات حدوث جرائم نظم المعلومات بمؤسساتهم

عدد مرات حدوث جرائم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
يومي على الأقل	16	11.3	23.5	23.5
أسبوعي على الأقل	2	1.4	2.9	26.5
شهري على الأقل	1	.7	1.5	27.9
سنوي على الأقل	13	9.2	19.1	47.1
غير منتظم	32	22.7	47.1	94.1
لا أدري	4	2.8	5.9	100.0
المجموع	68	48.2	100.0	

جدول رقم (17) يوضح استجابة عينة الدراسة (العاملين بالنظم) إزاء عدد الإنذارت بوجود جريمة عن طريق الإنترنت بمؤسساتهم

عدد الإنذارت بوجود جريمة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أقل من10	16	11.3	36.4	36.4
من 10 إلى أقل من 100	15	10.6	34.1	70.5
من 100إلى أقل من 1000	7	5.0	15.9	86.4
من 1000إلى أقل من 10000	3	2.1	6.8	93.2
من 10000إلى 50000	2	1.4	4.5	97.7
أكثر من 50000	1	.7	2.3	100.0
المجموع	44	68.8	100.0	

جدول رقم (18) يوضح استجابة عينة الدراسة (العاملين بالنظم، والموفرين) إزاء حجم استخدام أساليب ارتكاب جرائم نظم المعلومات مرتبة حسب حجم استخدامها

الأسلوب	العينة		المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
	العدد	لم يجب						
إرسال الفيروسات المدمرة بالبريد الإلكتروني أو برامج المحادثة وما شابهها	105	36	4.5238	5.0000	5.00	.9104	3.00	475
إرفاق أحصنة طروادة بالبرامج	105	36	4.2095	5.0000	5.00	.9776	3.00	442
النفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثورعلى ملفات مشاركة غير محمية	105	36	3.8667	5.0000	5.00	1.7269	4.00	406
محاولة اكتشاف المنافذ المفتوحة والدخول منها إلى الجهاز	105	36	3.7429	4.0000	4.00	1.1605	3.00	393
استغلال الثغرات التي تكتشف في نظم التشغيل والتطبيقات العاملة معه	105	36	3.7429	5.0000	5.00	1.6643	4.00	393
IP Spoofing	105	36	3.6476	4.0000	4.00	.9804	3.00	383
استغلال الثغرات الأمنية في مزودات Web Servers	105	36	3.5905	5.0000	5.00	1.8538	4.00	377
استخدام برامج حديثة تقوم بأستغلال نقاط الضعف في برامج الحماية	105	36	3.4952	4.0000	4.00	1.35252	4.00	367
استغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة	105	36	3.4667	4.0000	4.00	1.3521	4.00	364
ترك أقراص مرنة ملوثة بالفيروسات	105	36	3.1810	3.0000	3.00	.8060	4.00	334
برمجة النظم والتطبيقات بطريقة تحقق للمبرمج مصالح شخصية غير مشروعة	105	36	2.9429	4.0000	4.00	1.4400	3.00	309
سرقة وسائط الحفظ الخارجية نتيجة تساهل العاملين بالمنظمة	105	36	2.9333	3.0000	1.00	1.7112	4.00	308
التخفي تحت البرامج المجانية والمواقع الجذابة للحصول على معلومات عن الزائر	105	36	2.9048	3.0000	3.00	.9357	3.00	305
الاستخدام غير القانوني لأجهزة الغير حين تركها غير مؤمنة	105	36	2.7429	3.0000	4.00	1.3375	4.00	288
إرفاق الملفات (ذاتية التشغيل/ بحاجة إلى تشغيل) والتي تقوم بعمليات تخريبية	105	36	2.6857	3.0000	3.00	1.2035	3.00	282
انتحال شخصية عبر البريد الإلكتروني	105	36	2.6571	3.0000	4.00	1.2234	3.00	279
الحصول على البيانات السرية خلال أعمال صيانة الأجهزة	105	36	2.4571	3.0000	3.00	.9710	3.00	258
تشغيل الجهاز عن طريق القرص المرن للدخول الغير مرخص على الأقراص الثابتة والحصول على البيانات	105	36	2.2952	3.0000	3.00	.9600	2.00	241
زراعة برامج اختراق بواسطة موظفي الصيانة والتشغيل بالمنظمة	105	36	1.9810	2.0000	2.00	.8084	3.00	208

جدول رقم (18- أ) يوضح استجابتهم حيال حجم الإرسال الفيروسات المدمرة بالبريد الإلكتروني أو برامج المحادثة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	4	2.8	3.8	3.8
متوسط	18	12.8	17.1	21.0
عالي	2	1.4	1.9	22.9
عالي جداً	81	57.4	77.1	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ب) يوضح استجابتهم حيال حجم إرفاق أحصنة طروادة بالبرامج

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادر	10	7.1	9.5	9.5
متوسط	11	7.8	10.5	20.0
عالي	31	22.0	29.5	49.5
عالي جداً	53	37.6	50.5	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- جـ) يوضح استجابتهم حيال حجم النفاذ عبر الشبكة إلى الأجهزة المربوطة بها ومحاولة العثورعلى ملفات مشاركة غير محمية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	27	19.1	25.7	25.7
متوسط	1	.7	1.0	26.7
عالي	9	6.4	8.6	35.2
عالي جداً	68	48.2	64.8	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- د) يوضح استجابتهم حيال حجم استغلال الثغرات التي تكتشف في نظم التشغيل والتطبيقات العاملة معه

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	18	12.8	17.1	17.1
محدود	17	12.1	16.2	33.3
متوسط	2	1.4	1.9	35.2
عالي	5	3.5	4.8	40.0
عالي جداً	63	44.7	60.0	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- هـ) يوضح استجابتهم حيال حجم محاولة اكتشاف المنافذ المفتوحة والدخول منها إلى الجهاز

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	29	20.6	27.6	27.6
عالي	45	31.9	42.9	70.5
عالي جداً	31	22.0	29.5	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- و) يوضح استجابتهم حيال حجم IP Spoofing

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	18	12.8	17.1	17.1
متوسط	21	14.9	20.0	37.1
عالي	46	32.6	43.8	81.0
عالي جداً	20	14.2	19.0	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ز) يوضح استجابتهم حيال حجم استغلال الثغرات الأمنية في مزودات الويب

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	34	24.1	32.4	32.4
متوسط	5	3.5	4.8	37.1
عالي	2	1.4	1.9	39.0
عالي جداً	64	45.4	61.0	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ح) يوضح استجابتهم حيال حجم استخدام برامج حديثة تقوم بأستغلال نقاط الضعف في برامج الحماية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	7	5.0	6.7	6.7
محدود	31	22.0	29.5	36.2
عالي	37	26.2	35.2	71.4
عالي جداً	30	21.3	28.6	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ط) يوضح استجابتهم حيال حجم استغلال الثغرات التي تكتشف في برامج الحماية للنفاذ للأجهزة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	6	4.3	5.7	5.7
محدود	34	24.1	32.4	38.1
عالي	35	24.8	33.3	71.4
عالي جداً	30	21.3	28.6	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ي) يوضح استجابتهم حيال حجم ترك أقراص مرنة ملوثة بالفيروسات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	4	2.8	3.8	3.8
محدود	10	7.1	9.5	13.3
متوسط	58	41.1	55.2	68.6
عالي	29	20.6	27.6	96.2
عالي جداً	4	2.8	3.8	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ك) يوضح استجابتهم حيال حجم برمجة النظم والتطبيقات بطريقة تحقق للمبرمج مصالح شخصية غير مشروعة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	37	26.2	35.2	35.2
عالي	68	48.2	64.8	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ل) يوضح استجابتهم حيال حجم سرقة وسائط الحفظ الخارجية نتيجة تساهل العاملين بالمنظمة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	40	28.4	38.1	38.1
متوسط	28	19.9	26.7	64.8
عالي	1	.7	1.0	65.7
عالي جداً	36	25.5	34.3	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- م) يوضح استجابتهم حيال حجم التخفي تحت البرامج المجانية والمواقع الجذابة للحصول على معلومات عن الزائر

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	7	5.0	6.7	6.7
محدود	30	21.3	28.6	35.2
متوسط	34	24.1	32.4	67.6
عالي	34	24.1	32.4	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ن) يوضح استجابتهم حيال حجم ترك لاستخدام غير القانوني لأجهزة الغير حين تركها غير مؤمنة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	27	19.1	25.7	25.7
محدود	24	17.0	22.9	48.6
متوسط	8	5.7	7.6	56.2
عالي	41	29.1	39.0	95.2
عالي جداً	5	3.5	4.8	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- س) يوضح استجابتهم حيال حجم إرفاق الملفات (ذاتية التشغيل/ بحاجة إلى تشغيل) والتي تقوم بعمليات تخريبية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	30	21.3	28.6	28.6
محدود	7	5.0	6.7	35.2
متوسط	34	24.1	32.4	67.6
عالي	34	24.1	32.4	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ع) يوضح استجابتهم حيال حجم انتحال شخصية عبر البريد الإلكتروني

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	32	22.7	30.5	30.5
محدود	6	4.3	5.7	36.2
متوسط	33	23.4	31.4	67.6
عالي	34	24.1	32.4	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ف) يوضح استجابتهم حيال حجم الحصول على البيانات السرية خلال أعمال صيانة الأجهزة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	27	19.1	25.7	25.7
محدود	12	8.5	11.4	37.1
متوسط	57	40.4	54.3	91.4
عالي	9	6.4	8.6	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ص) يوضح استجابتهم حيال حجم ترك أقراص مرنة ملوثة بالفيروسات تشغيل الجهاز عن طريق القرص المرن للدخول الغير مرخص على الأقراص الثابتة والحصول على البيانات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	37	26.2	35.2	35.2
متوسط	68	48.2	64.8	100.0
المجموع	105	74.5	100.0	

جدول رقم (18- ق) يوضح استجابتهم حيال حجم زراعة برامج اختراق بواسطة موظفي الصيانة والتشغيل بالمؤسسة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	34	24.1	32.4	32.4
محدود	40	28.4	38.1	70.5
متوسط	30	21.3	28.6	99.0
عالي	1	.7	1.0	100.0
المجموع	105	74.5	100.0	

جدول رقم (19) يوضح استجابة عينة الدراسة (العاملين بالنظم) إزاء حجم استخدام المنافذ الداخلية والخارجية للمؤسسات في ارتكاب جرائم نظم المعلومات مرتبة حسب حجم استخدامها

المنفذ	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
عن طريق شبكة الانترنت	4.2500	5.00	5.00	1.2140	3.00	289
أفشاء الرقم السري	4.1618	5.00	5.00	1.1921	4.00	283
المحاولة المتكررة	3.9559	4.00	4.00	1.1121	4.00	269
عن طريق الأجهزة ومحركات الاقراص المرنة	3.9118	4.00	5.00	.9885	4.00	266
عن طريق الشبكة المحلية	3.8824	4.00	4.00	.7635	3.00	264
عن طريق الشبكة الواسعة	3.0588	3.00	4.00	1.0349	4.00	208
استخدام برامج فك التشفير	2.8824	3.00	4.00	1.2522	3.00	196
عن طريق شبكة VPN	2.4412	2.00	1.00	1.3201	3.00	166

جدول رقم (19- أ) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق شبكة الانترنت

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	14	9.9	20.6	20.6
متوسط	1	.7	1.5	22.1
عالي	7	5.0	10.3	32.4
عالي جداً	46	32.6	67.6	100.0
المجموع	68	48.2	100.0	

جدول رقم (19- ب) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق أفشاء الرقم السري

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	4	2.8	5.9	5.9
متوسط	19	13.5	27.9	33.8
عالي	3	2.1	4.4	38.2
عالي جداً	42	29.8	61.8	100.0
المجموع	68	48.2	100.0	

جدول رقم (19- جـ) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق المحاولة المتكررة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	4	2.8	5.9	5.9
محدود	5	3.5	7.4	13.2
متوسط	4	2.8	5.9	19.1
عالي	32	22.7	47.1	66.2
عالي جداً	23	16.3	33.8	100.0
المجموع	68	48.2	100.0	

جدول رقم (19- د) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق الأجهزة ومحركات الاقراص المرنة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	1	.7	1.5	1.5
محدود	3	2.1	4.4	5.9
متوسط	21	14.9	30.9	36.8
عالي	19	13.5	27.9	64.7
عالي جداً	24	17.0	35.3	100.0
المجموع	68	48.2	100.0	

جدول رقم (19- هـ) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق الشبكة المحلية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	2	1.4	2.9	2.9
متوسط	18	12.8	26.5	29.4
عالي	34	24.1	50.0	79.4
عالي جداً	14	9.9	20.6	100.0
المجموع	68	48.2	100.0	

جدول رقم (19- و) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق الشبكة الواسعة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	4	2.8	5.9	5.9
محدود	19	13.5	27.9	33.8
متوسط	17	12.1	25.0	58.8
عالي	25	17.7	36.8	95.6
عالي جداً	3	2.1	4.4	100.0
المجموع	68	48.2	100.0	

جدول رقم (19- ز) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق استخدام برامج فك التشفير

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	18	12.8	26.5	26.5
محدود	3	2.1	4.4	30.9
متوسط	16	11.3	23.5	54.4
عالي	31	22.0	45.6	100.0
المجموع	68	48.2	100.0	

جدول رقم (19- ح) يوضح استجابتهم حيال حجم ارتكاب الجرائم عن طريق شبكة VPN

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	25	17.7	36.8	36.8
محدود	13	9.2	19.1	55.9
متوسط	5	3.5	7.4	63.2
عالي	25	17.7	36.8	100.0
المجموع	68	48.2	100.0	

جدول رقم (20) يوضح استجابة عينة الدراسة (العاملين بالنظم، والموفرين) إزاء حجم استخدام الإدوات التقنية في ارتكاب جرائم نظم المعلومات مرتبة حسب حجم استخدامها

الأدوات	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
الفيروسات وديدان الإنترنت	4.5333	5.000	5.00	.7974	2.00	476.0
cookies	4.5143	5.000	5.00	.6667	2.00	474.0
البريد الإلكتروني	4.1810	5.000	5.00	.9280	2.00	439.0
المشاركة في الملفات على الشبكة	4.0762	4.000	5.00	.9374	3.00	428.0
برامج التنصت على الشبكات	3.8857	4.000	3.00	.9539	3.00	408.0
Net Bus	3.8000	4.000	4.00	1.1215	4.00	399.0
Sub Seven	3.7524	4.000	4.00	1.1912	4.00	394.0
ICQ	3.5143	3.000	3.00	1.1938	3.00	369.0
Password Recovery Toolkit	3.4667	4.000	2.00	1.1935	3.00	364.0
Tribe Flood Network(TFN)	3.2857	3.000	3.00	1.1242	3.00	345.0
Hack a Tack	3.1905	3.000	2.00	1.0750	4.00	335.0
Win Crash	3.1619	3.000	3.00	.8784	3.00	332.0
أقراص بدء التشغيل	3.0095	3.000	3.00	.6722	2.00	316.0
MS Word Cracker	3.0095	3.000	3.00	.9354	3.00	316.0
MS Excel Cracker	2.8857	3.000	3.00	.7508	3.00	303.0
Caligula	2.7619	3.000	2.00	.9357	3.00	290.0
Marker Groove	2.7143	3.000	2.00	.9579	3.00	285.0
Revelation	2.4095	2.000	2.00	.6154	3.00	253.0

جدول رقم (20- أ) يوضح استجابتهم حيال حجم استخدام الفيروسات وديدان الإنترنت

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوسط	20	14.2	19.0	19.0
عالي	9	6.4	8.6	27.6
عالي جداً	76	53.9	72.4	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ب) يوضح استجابتهم حيال حجم استخدام cookies

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوسط	10	7.1	9.5	9.5
عالي	31	22.0	29.5	39.0
عالي جداً	64	45.4	61.0	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- جـ) يوضح استجابتهم حيال حجم استخدام البريد الإلكتروني

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوسط	37	26.2	35.2	35.2
عالي	12	8.5	11.4	46.7
عالي جداً	56	39.7	53.3	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- د) يوضح استجابتهم حيال حجم استخدام المشاركة في الملفات على الشبكة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	6	4.3	5.7	5.7
متوسط	24	17.0	22.9	28.6
عالي	31	22.0	29.5	58.1
عالي جداً	44	31.2	41.9	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- هـ) يوضح استجابتهم حيال حجم استخدام برامج التنصت على الشبكات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	5	3.5	4.8	4.8
متوسط	39	27.7	37.1	41.9
عالي	24	17.0	22.9	64.8
عالي جداً	37	26.2	35.2	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- و) يوضح استجابتهم حيال حجم استخدام Net Bus

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	2	1.4	1.9	1.9
محدود	19	13.5	18.1	20.0
متوسط	9	6.4	8.6	28.6
عالي	43	30.5	41.0	69.5
عالي جداً	32	22.7	30.5	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ز) يوضح استجابتهم حيال حجم استخدام Sub Seven

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	2	1.4	1.9	1.9
محدود	24	17.0	22.9	24.8
متوسط	6	4.3	5.7	30.5
عالي	39	27.7	37.1	67.6
عالي جداً	34	24.1	32.4	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ح) يوضح استجابتهم حيال حجم استخدام ICQ

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	24	17.0	22.9	22.9
متوسط	40	28.4	38.1	61.0
عالي	4	2.8	3.8	64.8
عالي جداً	37	26.2	35.2	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ط) يوضح استجابتهم حيال حجم استخدام Password Recovery Toolkit

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	35	24.8	33.3	33.3
متوسط	12	8.5	11.4	44.8
عالي	32	22.7	30.5	75.2
عالي جداً	26	18.4	24.8	100.0
المجموع	105	74.5	100.0	
لم يجب	36	25.5		
المجموع الكللي	141	100.0		

جدول رقم (20- ي) يوضح استجابتهم حيال حجم استخدام Tribe Flood Network (TFN)

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	32	22.7	30.5	30.5
متوسط	34	24.1	32.4	62.9
عالي	16	11.3	15.2	78.1
عالي جداً	23	16.3	21.9	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ك) يوضح استجابتهم حيال حجم استخدام Hack a Tack

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	2	1.4	1.9	1.9
محدود	34	24.1	32.4	34.3
متوسط	23	16.3	21.9	56.2
عالي	34	24.1	32.4	88.6
عالي جداً	12	8.5	11.4	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ل) يوضح استجابتهم حيال حجم استخدام Win Crash

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	27	19.1	25.7	25.7
متوسط	40	28.4	38.1	63.8
عالي	32	22.7	30.5	94.3
عالي جداً	6	4.3	5.7	100.0
المجموع	105	74.5	100.0	
لم يجب	36	25.5		
المجموع الكللي	141	100.0		

جدول رقم (20- م) يوضح استجابتهم حيال حجم استخدام أقراص بدء التشغيل

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	23	16.3	21.9	21.9
متوسط	58	41.1	55.2	77.1
عالي	24	17.0	22.9	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- س) يوضح استجابتهم حيال حجم استخدام MS Word Cracker

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	35	24.8	33.3	33.3
متوسط	44	31.2	41.9	75.2
عالي	16	11.3	15.2	90.5
عالي جداً	10	7.1	9.5	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ع) يوضح استجابتهم حيال حجم استخدام MS Excel Cracker

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	34	24.1	32.4	32.4
متوسط	51	36.2	48.6	81.0
عالي	18	12.8	17.1	98.1
عالي جداً	2	1.4	1.9	100.0
المجموع	105	74.5	100.0	
لم يجب	36	25.5		
المجموع الكللي	141	100.0		

جدول رقم (20- ف) يوضح استجابتهم حيال حجم استخدام Caligula

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	8	5.7	7.6	7.6
محدود	37	26.2	35.2	42.9
متوسط	32	22.7	30.5	73.3
عالي	28	19.9	26.7	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ص) يوضح استجابتهم حيال حجم استخدام Marker Groove

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	10	7.1	9.5	9.5
محدود	37	26.2	35.2	44.8
متوسط	31	22.0	29.5	74.3
عالي	27	19.1	25.7	100.0
المجموع	105	74.5	100.0	

جدول رقم (20- ق) يوضح استجابتهم حيال حجم استخدام Revelation

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يستخدم	1	.7	1.0	1.0
محدود	66	46.8	62.9	63.8
متوسط	32	22.7	30.5	94.3
عالي	6	4.3	5.7	100.0
المجموع	105	74.5	100.0	

جدول رقم (21) يوضح استجابة عينة الدراسة (العاملين بالنظم، والموفرين) إزاء حجم الحصول على إدوات ارتكاب جرائم النظم

طريقة الحصول عليها	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
البرامج المجانية التي يتم الحصول عليها من مواقع على شبكة الإنترنت	4.962	5.000	5.00	.1923	1.00	521.0
أما كن بيع البرامج الغير قانونية	4.714	5.000	5.00	.4539	1.00	495.0
البرامج الغير مجانية التي تشترى من مواقع على شبكة الإنترنت	3.667	4.000	4.00	.4737	1.00	385.0
محلات بيع البرامج المرخصة	2.571	3.000	3.00	1.0639	3.00	270.0

جدول رقم (21- أ) يوضح استجابتهم حيال حجم البرامج المجانية التي يتم الحصول عليها من مواقع على شبكة الإنترنت

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
عالي	4	2.8	3.8	3.8
عالي جداً	101	71.6	96.2	100.0
المجموع	105	74.5	100.0	

جدول رقم (21- ب) يوضح استجابتهم حيال حجم الحصول عليها من أما كن بيع البرامج الغير قانونية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
عالي	30	21.3	28.6	28.6
عالي جداً	75	53.2	71.4	100.0
المجموع	105	74.5	100.0	

جدول رقم (21- جـ) يوضح استجابتهم حيال حجم البرامج الغير مجانية التي تشترى من مواقع على شبكة الإنترنت

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوسط	35	24.8	33.3	33.3
عالي	70	49.6	66.7	100.0
المجموع	105	74.5	100.0	

جدول رقم (21- د) يوضح استجابتهم حيال حجم الحصول عليها من محلات بيع البرامج المرخصة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا أدري	28	19.9	26.7	26.7
محدود	7	5.0	6.7	33.3
متوسط	52	36.9	49.5	82.9
عالي	18	12.8	17.1	100.0
المجموع	105	74.5	100.0	

جدول رقم (22) يوضح استجابة عينة (المحققين، والعاملين بالنظم) تجاه مستوى مكافحة جرائم نظم المعلومات

	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
قدر الجهد المبذول لمتابعة جرائم نظم المعلومات من قبل قسم خاص	3.96	4.00	5	1.13	3	396
الاعتماد على ضمانات موردي الأجهزة والبرامج بدلاً من تتبع الجرائم	3.38	3.00	3	.66	3	351
جرائم نظم المعلومات التي اكتشفت وضبطت ملابساتها	3.06	3.00	3	.79	3	318
الجرائم التي تم ضبطها ومعرفة مصدرها وآثارها في المنظمة	3.04	3.00	3	.81	3	316
حجم أهتمام الجهة الأمنية بعد الإبلاغ عن الجريمة المعلوماتية	2.88	3.00	4	1.29	4	299
جرائم نظم المعلومات التي اكتشفت دون ضبط ملابساتها	2.63	3.00	3	.81	3	273

جدول رقم (22- أ) يوضح استجابتهم نحو قدر الجهد المبذول لمتابعة جرائم نظم المعلومات من قبل قسم خاص

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	20	14.2	20.0	20.0
متوسط	5	3.5	5.0	25.0
عالي	34	24.1	34.0	59.0
عالي جداً	41	29.1	41.0	100.0
المجموع	100	70.9	100.0	
لم يستجيبوا	4	2.8		

جدول رقم (22- ب) يوضح استجابتهم نحو الاعتماد على ضمانات موردي الأجهزة والبرامج بدلاً من تتبع الجرائم

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	8	5.7	7.7	7.7
متوسط	51	36.2	49.0	56.7
عالي	43	30.5	41.3	98.1
عالي جداً	2	1.4	1.9	100.0
المجموع	104	73.8	100.0	

جدول رقم (22- جـ) يوضح استجابتهم نحو جرائم نظم المعلومات التي اكتشفت وضبطت ملابساتها

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	3	2.1	2.9	2.9
محدود	20	14.2	19.2	22.1
متوسط	49	34.8	47.1	69.2
عالي	32	22.7	30.8	100.0
المجموع	104	73.8	100.0	

جدول رقم (22- د) يوضح استجابتهم نحو الجرائم التي تم ضبطها ومعرفة مصدرها وآثارها في المؤسسة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	2	1.4	1.9	1.9
محدود	26	18.4	25.0	26.9
متوسط	42	29.8	40.4	67.3
عالي	34	24.1	32.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (22- هـ) يوضح استجابتهم نحو حجم أهتمام الجهة الأمنية بعد الإبلاغ عن الجريمة المعلوماتية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	19	13.5	18.3	18.3
محدود	27	19.1	26.0	44.2
متوسط	15	10.6	14.4	58.7
عالي	34	24.1	32.7	91.3
عالي جداً	9	6.4	8.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (22- و) يوضح استجابتهم نحو جرائم نظم المعلومات التي اكتشفت دون ضبط ملابساتها

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	10	7.1	9.6	9.6
محدود	31	22.0	29.8	39.4
متوسط	51	36.2	49.0	88.5
عالي	12	8.5	11.5	100.0
المجموع	104	73.8	100.0	

جدول رقم (23) يوضح استجابة عينة (المحققين، والعاملين بالنظم) تجاه أسباب ودوافع ارتكاب جرائم نظم المعلومات

الدافع	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
تسلية وحب استطلاع	4.192	4.0000	5.00	.9459	4.00	436
الوصول إلى معلومات شخصية	4.058	4.0000	5.00	.9536	3.00	422
إبراز قدرات	4.019	4.0000	5.00	.9449	3.00	418
انتقام	3.981	4.5000	5.00	1.3364	4.00	414
أقتصادية وتجارية	3.250	4.0000	4.00	1.0950	4.00	338
سياسية وعسكرية	2.135	2.0000	1.00	1.2927	3.00	222

جدول رقم (23- أ) يوضح استجابة عينة الدراسة تجاه تقييمهم لدافع التسلية وحب الاستطلاع

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	3	2.1	2.9	2.9
متوسط	20	14.2	19.2	22.1
عالي	32	22.7	30.8	52.9
عالي جداً	49	34.8	47.1	100.0
المجموع	104	73.8	100.0	

جدول رقم (23- ب) يوضح استجابة عينة الدراسة تجاه تقييمهم لدافع الوصول إلى معلومات شخصية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	6	4.3	5.8	5.8
متوسط	26	18.4	25.0	30.8
عالي	28	19.9	26.9	57.7
عالي جداً	44	31.2	42.3	100.0
المجموع	104	73.8	100.0	

جدول رقم (23- جـ) يوضح استجابة عينة الدراسة تجاه تقييمهم لدافع إبراز قدرات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدود	7	5.0	6.7	6.7
متوسط	24	17.0	23.1	29.8
عالي	33	23.4	31.7	61.5
عالي جداً	40	28.4	38.5	100.0
المجموع	104	73.8	100.0	

جدول رقم (23- د) يوضح استجابة عينة الدراسة تجاه تقييمهم لدافع الانتقام

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	12	8.5	11.5	11.5
محدود	3	2.1	2.9	14.4
متوسط	12	8.5	11.5	26.0
عالي	25	17.7	24.0	50.0
عالي جداً	52	36.9	50.0	100.0
المجموع	104	73.8	100.0	

جدول رقم (23- هـ) يوضح استجابة عينة الدراسة تجاه تقييمهم لدافع الأقتصادي والتجاري

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	8	5.7	7.7	7.7
محدود	22	15.6	21.2	28.8
متوسط	16	11.3	15.4	44.2
عالي	52	36.9	50.0	94.2
عالي جداً	6	4.3	5.8	100.0
المجموع	104	73.8	100.0	

جدول رقم (23- و) يوضح استجابة عينة الدراسة تجاه تقييمهم لدافع سياسية وعسكرية

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	51	36.2	49.0	49.0
محدود	17	12.1	16.3	65.4
متوسط	7	5.0	6.7	72.1
عالي	29	20.6	27.9	100.0
المجموع	104	73.8	100.0	

جدول رقم (24) يوضح استجابة عينة العاملين بالنظم تجاه تقييمهم لتكلفة جرائم نظم المعلومات بمؤسساتهم

العنصر	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أقل من 5 بالمائة	29	20.6	42.6	42.6
من 5 بالمائة ألى أقل من 10 بالمائة	25	17.7	36.8	79.4
من 10 بالمائة ألى أقل من 30 بالمائة	10	7.1	14.7	94.1
من 30 بالمائة ألى 50 بالمائة	3	2.1	4.4	98.5
أكثر من 50 بالمائة	1	.7	1.5	100.0
المجموع	68	48.2	100.0	

جدول رقم (25) يوضح استجابة عينة (المحققين، والعاملين بالنظم) لمدى أمكانية تحديد مصدر وأدوات الهجوم

العنصر	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
تستطيع المنظمة المستهدفة من قبل مجرمي نظم (المعلومات تحديد مصدر الهجوم (داخلي، خارجي	3.9038	4.000	4.00	.8187	3.00	406
تستطيع المنظمة المستهدفة من قبل مجرمي نظم المعلومات تحديد الأدوات المستخدمة بالهجوم	3.1923	3.000	3.00	1.0247	3.00	332

جدول رقم (25- أ) يوضح استجابة عينة الدراسة إزاء لمدىاستطاعة المؤسسة المستهدفة من قبل مجرمي نظم المعلومات بتحديد مصدر الهجوم

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	8	5.7	7.7	7.7
أحياناً	16	11.3	15.4	23.1
غالباً	58	41.1	55.8	78.8
دائماً	22	15.6	21.2	100.0
المجموع	104	73.8	100.0	

جدول رقم (25- ب) يوضح استجابة عينة الدراسة إزاء لمدى استطاعة المؤسسة المستهدفة من قبل مجرمي نظم المعلومات بتحديد الأدوات المستخدمة بالهجوم

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	32	22.7	30.8	30.8
أحياناً	34	24.1	32.7	63.5
غالباً	24	17.0	23.1	86.5
دائماً	14	9.9	13.5	100.0
المجموع	104	73.8	100.0	

جدول رقم (26) يوضح استجابة عينة (المحققين، والعاملين بالنظم) لمدى أمكانية ستخدام القنية كوسيلة ضبط وتحقيق

العنصر	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
من الممكن استخدام تقنية المعلومات كوسيلة من وسائل ضبط الجريمة والتحقيق فيها	4.1635	4.000	4.00	.7388	3.00	433
يمكن اعتبار برامج الحماية وسيلة ضبط وتحقيق هامة	4.5096	5.000	5.00	.6967	2.00	469

جدول رقم (26- أ) يظهر استجابة عينة الدراسة حيال أمكانية استخدام تقنية المعلومات كوسيلة من وسائل ضبط الجريمة والتحقيق فيها

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
نادراً	4	2.8	3.8	3.8
أحياناً	9	6.4	8.7	12.5
غالباً	57	40.4	54.8	67.3
دائماً	34	24.1	32.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (26- ب) يظهر استجابة عينة الدراسة حيال أمكانية استخدام اعتبار برامج الحماية وسيلة ضبط وتحقيق هامة

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
أحياناً	12	8.5	11.5	11.5
غالباً	27	19.1	26.0	37.5
دائماً	65	46.1	62.5	100.0
المجموع	104	73.8	100.0	

جدول رقم (27) يوضح استجابة عينة (المحققين، والعاملين بالنظم) إزاء مدى مساعدة برامج الحماية بضبط الجريمة كأحد الوسائل المستخدمة بالتحقيق

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
تحديد نوع الجريمة المرتكبة	1	.7	1.0	1.0
تحديد توقيت ارتكابب الجريمة	2	1.4	1.9	2.9
تحديد مصدر الجريمة	3	2.1	2.9	5.8
الإعلام بوجود جريمة مرتكبة	1	.7	1.0	6.7
تحديد نوع الجريمة وتوقيت ارتكابها	5	3.5	4.8	11.5
تحديد نوعها ومصدرها وتوقيت ارتكابها والإعلام بوجودها	75	53.2	72.1	83.7
تحديد نوع الجريمة وتوقيت ارتكابها والإعلام بوجود جريمة مرتكبه	17	12.1	16.3	100.0
المجموع	104	73.8	100.0	

جدول رقم (28) يوضح استجابة عينة (المحققين، والعاملين بالنظم، الموفرين) حول تقييمهم لمدى أهمية الأدوات التي يمكن استخدامها بضبط الجريمة

أدوات الضبط	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
سجل الصلاحيات للمستخدمين	4.9433	5.00	5.00	.2322	1.00	697
التقارير التي تنتجها نظم أمن البيانات Reporting	4.8582	5.00	5.00	.3501	1.00	685
برامج النسخ الاحتياطي والتسجيل Logging	4.7589	5.00	5.00	.4293	1.00	671
برامج كشف الفيروسات	4.7447	5.00	5.00	.4376	1.00	669
أدوات المراجعة Auditing	4.6879	5.00	5.00	.4650	1.00	661
تقارير الجدران النارية Reporting	4.5319	5.00	5.00	.5419	2.00	639
أدوات مراقبة المستخدمين للشبكة	4.5248	5.00	5.00	.6717	2.00	638
برامج تتبع المخترقين	4.1135	4.00	5.00	.8709	3.00	580
مراجعة قاعدة البيانات	4.0780	4.00	4.00	.7375	2.00	575
برامج تتبع مصدر الرسائل	4.0638	4.00	5.00	.9503	3.00	573

جدول رقم (28- أ) يظهر استجابة عينة الدراسة حيال أهمية سجل الصلاحيات للمستخدمين كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم	8	5.7	5.7	5.7
مهم جداً	133	94.3	94.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- ب) يظهر استجابة عينة الدراسة حيال أهمية التقارير التي تنتجها نظم أمن البيانات كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم	20	14.2	14.2	14.2
مهم جداً	121	85.8	85.8	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- جـ) يظهر استجابة عينة الدراسة حيال أهمية برامج النسخ الاحتياطي والتسجيل كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم	34	24.1	24.1	24.1
مهم جداً	107	75.9	75.9	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- د) يظهر استجابة عينة الدراسة حيال أهمية برامج كشف الفيروسات كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم	36	25.5	25.5	25.5
مهم جداً	105	74.5	74.5	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- هـ) يظهر استجابة عينة الدراسة حيال أهمية أدوات المراجعة كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم	44	31.2	31.2	31.2
مهم جداً	97	68.8	68.8	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- و) يظهر استجابة عينة الدراسة حيال أهمية تقارير الجدران النارية كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم إلى حدٍ ما	3	2.1	2.1	2.1
مهم	60	42.6	42.6	44.7
مهم جداً	78	55.3	55.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- ز) يظهر استجابة عينة الدراسة حيال أهمية أدوات مراقبة المستخدمين للشبكة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم إلى حدٍ ما	14	9.9	9.9	9.9
مهم	39	27.7	27.7	37.6
مهم جداً	88	62.4	62.4	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- ح) يظهر استجابة عينة الدراسة حيال أهمية برامج تتبع المخترقين كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	3	2.1	2.1	2.1
مهم إلى حدٍ ما	37	26.2	26.2	28.4
مهم	42	29.8	29.8	58.2
مهم جداً	59	41.8	41.8	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- ط) يظهر استجابة عينة الدراسة حيال أهمية مراجعة قاعدة البيانات كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
مهم إلى حدٍ ما	33	23.4	23.4	23.4
مهم	64	45.4	45.4	68.8
مهم جداً	44	31.2	31.2	100.0
المجموع	141	100.0	100.0	

جدول رقم (28- ي) يظهر استجابة عينة الدراسة حيال أهمية برامج تتبع مصدر الرسائل كأداة ضبط

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	11	7.8	7.8	7.8
مهم إلى حدٍ ما	26	18.4	18.4	26.2
مهم	47	33.3	33.3	59.6
مهم جداً	57	40.4	40.4	100.0
المجموع	141	100.0	100.0	

جدول رقم (29) يوضح استجابة عينة (المحققين، والعاملين بالنظم) حول مدى مساهمة الوسائل التالية في التعرف على شخصية مرتكب جريمة نظم المعلومات

يمكن التعرف على شخصية مرتكب جريمة نظم المعلومات بالمؤسسة بواسطة	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
عنوان IP	5	3.5	4.8	4.8
برامج الحماية	3	2.1	2.9	7.7
وسائل تتبع المخترقين	2	1.4	1.9	9.6
برامج تتبع مصدر الرسائل	1	.7	1.0	10.6
عنوانIP + برامج الحماية	11	7.8	10.6	21.2
عنوانIP + استخدام وسائل تتبع المخترقين برامج الحماية	21	14.9	20.2	41.3
عنوانIP + برامج الحماية + تتبع المخترقين تتبع مصدر الرسائل	56	39.7	53.8	95.2
عنوانIP + برامج الحماية + تتبع مصدر الرسائل	5	3.5	4.8	100.0
المجموع	104	73.8	100.0	

جدول رقم (30) يوضح استجابة عينة (المحققين، والعاملين بالنظم) حول مدى مساعدة برامج الحماية في التحقيق

يمكن ضبط جريمة نظم المعلومات بالمؤسسة باستخدام	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
وسائل أمن البيانات	21	14.9	20.2	20.2
تعقب إجراءات أمن العاملين	12	8.5	11.5	31.7
وسائل أمن البيانات و تتبع إجراءات أمن العاملين	71	50.4	68.3	100.0
المجموع	104	73.8	100.0	

جدول رقم (31) يوضح استجابة عينة (المحققين، والعاملين بالنظم، الموفرين) حول تقييمهم لمدى أهمية الأدوات التي يمكن استخدامها كأدوات تساعد بالتحقيق في جرائم نظم المعلومات

الأداة المساعدة بالتحقيق	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
أداة فك التشفير	3.9574	4.00	4.00	.9847	3.00	558
برامج كسر كلمة المرور	3.9362	4.00	3.00	.9578	4.00	555
أدوات استرجاع المعلومات من الأقراص التالفة	3.9220	3.00	3.00	1.0076	3.00	553
برامج مقارنة النسخ	3.7801	4.00	4.00	.8627	3.00	533
برامج تشغيل الحاسب	3.2979	3.00	3.00	.5175	2.00	465
برامج البحث عن الملفات العادية والمخفية مثل	3.1844	3.00	4.00	.8071	3.00	449
برامج نسخ البيانات مثل Lap link	3.0496	3.00	3.00	.5648	2.00	430
برامج الضغط وفك الضغط Pkzip	3.0213	3.00	3.00	.7603	3.00	426
برامج اتصالات	2.5290	2.00	2.00	.9977	3.00	349

جدول رقم (31- أ) يوضح تقييم العينة لأداة فك التشفير

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	19	13.5	13.5	13.5
مهم إلى حدٍ ما	14	9.9	9.9	23.4
مهم	62	44.0	44.0	67.4
مهم جداً	46	32.6	32.6	100.0
Total	141	100.0	100.0	

جدول رقم (31- ب) يوضح تقييم العية لبرامج كسر كلمة المرور

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم إطلاقاً	3	2.1	2.1	2.1
مهم إلى حدٍ ما	51	36.2	36.2	38.3
مهم	36	25.5	25.5	63.8
مهم جداً	51	36.2	36.2	100.0
المجموع	141	100.0	100.0	

جدول رقم (31- جـ) يوضح تقييم العينة لأدوات استرجاع المعلومات من الأقراص التالفة مثل Viewdisk

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	3	2.1	2.1	2.1
مهم إلى حدٍ ما	68	48.2	48.2	50.4
مهم	7	5.0	5.0	55.3
مهم جداً	63	44.7	44.7	100.0
المجموع	141	100.0	100.0	

جدول رقم (31– د) يوضح تقييم العينة لبرامج مقارنة النسخ

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	10	7.1	7.1	7.1
مهم إلى حدٍ ما	41	29.1	29.1	36.2
مهم	60	42.6	42.6	78.7
مهم جداً	30	21.3	21.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (31- هـ) يوضح تقييم العينة لبرامج تشغيل الحاسب مثل Bootable diskette

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	4	2.8	2.8	2.8
مهم إلى حدٍ ما	91	64.5	64.5	67.4
مهم	46	32.6	32.6	100.0
المجموع	141	100.0	100.0	

جدول رقم (31– و) يوضح تقييم العينة لبرامج البحث عن الملفات العادية والمخفية Xtreepro gold

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم إطلاقاً	3	2.1	2.1	2.1
غير مهم	26	18.4	18.4	20.6
مهم إلى حدٍ ما	54	38.3	38.3	58.9
مهم	58	41.1	41.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (31- ز) يوضح تقييم العينة لبرامج نسخ البيانات مثل Lap link

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	19	13.5	13.5	13.5
مهم إلى حدٍ ما	96	68.1	68.1	81.6
مهم	26	18.4	18.4	100.0
المجموع	141	100.0	100.0	

جدول رقم (31- ح) يوضح تقييم العينة لبرامج الضغط وفك الضغط Pkzip

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم إطلاقاً	10	7.1	7.1	7.1
غير مهم	9	6.4	6.4	13.5
مهم إلى حدٍ ما	90	63.8	63.8	77.3
مهم	32	22.7	22.7	100.0
المجموع	141	100.0	100.0	

جدول رقم (31– ط) يوضح تقييم العينة لبرامج اتصالات مثل Lantastic

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم إطلاقاً	21	14.9	15.2	15.2
غير مهم	53	37.6	38.4	53.6
مهم إلى حدٍ ما	34	24.1	24.6	78.3
مهم	30	21.3	21.7	100.0
المجموع	138	97.9	100.0	
لم يستجيبوا	3	2.1		
المجموع الكلي	141	100.0		

جدول رقم (32) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، وموفري التقنيات) عوائق التحقيق المتعلقة بعدم وجود تشريع

	عدم وحود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد
المتوسط	4.6312
الوسيط	5.0000
المنوال	5.00
الانحراف المعياري	.5783
المدى	2.00
المجموع	653.00

جدول رقم (32- أ) يوضح استجابة العينة حول عدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
موافق إلى حدٍ ما	7	5.0	5.0	5.0
موافق	38	27.0	27.0	31.9
موافق بشدة	96	68.1	68.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (33) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، وموفري التقنيات) عوائق التحقيق المتعلقة بالجريمة مرتبة حسب أهميتها

معوقات متعلقة بالجريمة	مكونات عناصر جريمة نظم المعلومات غير معروفة للأطراف المعنية بالجريمة	إمكانية ارتكاب هذه الجرائم عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط
المتوسط	3.5603	1.9504
الوسيط	4.0000	2.0000
المنوال	3.00	2.00
الانحراف المعياري	.5778	.7867
المدى	2.00	3.00
المجموع	502.00	275.00

جدول رقم (33- أ) يوضح مكونات عناصر جريمة نظم المعلومات غير معروفة للأطراف المعنية بالجريمة

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
موافق إلى حدٍ ما	68	48.2	48.2	48.2
موافق	67	47.5	47.5	95.7
موافق بشدة	6	4.3	4.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (33- ب) إمكانية ارتكاب هذه الجرائم عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق بشدة	34	24.1	24.1	24.1
غير موافق	93	66.0	66.0	90.1
موافق إلى حدٍ ما	1	.7	.7	90.8
موافق	13	9.2	9.2	100.0
المجموع	141	100.0	100.0	

جدول رقم (34) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم، وموفري التقنيات) نحو تقييمهم لمعوقات التحقيق المتعلقة بالجهات المتضررة مرتبة حسب أهميتها

معوقات التحقيق المتعلقة بالجهات المتضررة	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى	المجموع
معظم المؤسسات المتضررة من جرائم نظم المعلومات لا تتقدم بشكوى للجهات الرسمية	4.085	4.00	5.00	.8576	2.00	576.00
عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين	3.851	4.00	4.00	.7832	3.00	543.00
مقاومة الموظفين الوسائل الأمنية للإبقاء على قدر من الحرية	3.830	4.00	4.00	.6650	2.00	540.00
لا توجد قناعة لدى العاملين في مجال نظم المعلومات بتدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية	3.830	3.00	4.00	1.3467	4.00	427.00
عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق	3.482	3.00	3.00	.6612	3.00	491.00
عدم وجود مردود مادي ملحوظ لتحديث برامج الحماية والتحقيق	3.099	4.00	4.00	.9878	2.00	437.00
لا توجد متابعة للمستجدات حول جرائم نظم المعلومات	2.936	3.00	3.00	.5633	3.00	414.00
لا يوجد قسم متخصص في جرائم المعلوماتية لديكم	2.887	3.00	2.00	1.0829	3.00	407.00
لا تتم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات	2.745	2.00	2.00	1.4462	4.00	387.00
تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية	2.121	2.00	2.00	.9671	4.00	299.00

جدول رقم (34- أ) يوضح مدى موافقة العينة حيال معوق معظم المؤسسات المتضررة من جرائم نظم المعلومات لا تتقدم بشكوى للجهات الرسمية

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
موافق إلى حدٍ ما	46	32.6	32.6	32.6
موافق	37	26.2	26.2	58.9
موافق بشدة	58	41.1	41.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- ب) يوضح مدى موافقة العينة حيال معوق عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق	7	5.0	5.0	5.0
موافق إلى حدٍ ما	34	24.1	24.1	29.1
موافق	73	51.8	51.8	80.9
موافق بشدة	27	19.1	19.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- جـ) يوضح مدى موافقة العينة حيال معوق مقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
موافق إلى حدٍ ما	45	31.9	31.9	31.9
موافق	75	53.2	53.2	85.1
موافق بشدة	21	14.9	14.9	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- د) يوضح مدى موافقة العينة حيال معوق عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق	7	5.0	5.0	5.0
موافق إلى حدٍ ما	65	46.1	46.1	51.1
موافق	63	44.7	44.7	95.7
موافق بشدة	6	4.3	4.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- هـ) يوضح مدى موافقة العينة حيال معوق عدم وجود مردود مادي ملحوظ لتحديث برامج الحماية والتحقيق

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق	62	44.0	44.0	44.0
موافق إلى حدٍ ما	3	2.1	2.1	46.1
موافق	76	53.9	53.9	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- و) يوضح مدى موافقة العينة حيال معوق عدم قناعة العاملين في مجال نظم المعلومات بتدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق بشدة	34	24.1	24.1	24.1
غير موافق	9	6.4	6.4	30.5
موافق إلى حدٍ ما	31	22.0	22.0	52.5
موافق	53	37.6	37.6	90.1
موافق بشدة	14	9.9	9.9	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- ز) يوضح مدى موافقة العينة حيال معوق عدم متابعة المستجدات حول جرائم نظم المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق	21	14.9	14.9	14.9
موافق إلى حدٍ ما	114	80.9	80.9	95.7
موافق بشدة	6	4.3	4.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- ح) يوضح مدى موافقة العينة حيال معوق عدم وجود قسم متخصص في جرائم المعلوماتية لديكم

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق	68	48.2	48.2	48.2
موافق إلى حدٍ ما	44	31.2	31.2	79.4
موافق	6	4.3	4.3	83.7
موافق بشدة	23	16.3	16.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- ط) يوضح مدى موافقة العينة حيال معوق عدم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق بشدة	34	24.1	24.1	24.1
غير موافق	37	26.2	26.2	50.4
موافق إلى حدٍ ما	31	22.0	22.0	72.3
موافق	9	6.4	6.4	78.7
موافق بشدة	30	21.3	21.3	100.0
المجموع	141	100.0	100.0	

جدول رقم (34- ي) يوضح مدى موافقة العينة حيال معوق عدم تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير موافق بشدة	33	23.4	23.4	23.4
غير موافق	80	56.7	56.7	80.1
موافق إلى حدٍ ما	9	6.4	6.4	86.5
موافق	16	11.3	11.3	97.9
موافق بشدة	3	2.1	2.1	100.0
المجموع	141	100.0	100.0	

جدول رقم (35) يوضح استجابة عينة المحققين حيال مدى توفر الكفاءة البشرية القادرة على التحقيق في جرائم نظم المعلومات

العنصر	المتوسط	الوسيط	المنوال	الانحراف المعياري	المجموع	Sum
المهارة العالية لاستخدام الحاسب الآلي والإنترنت	2.92	3.00	2.00	1.0790	4.00	105
المعرفة بمتطلبات أمن المعلومات	2.42	2.00	2.00	.9373	4.00	87.00
المقدرة على إتباع السياسة الأمنية للتعامل مع الجرائم	3.17	3.00	3.00	.8452	4.00	114
المعرفة بأساليب ارتكاب جرائم نظم المعلومات	2.28	2.00	2.00	.7411	3.00	82.00
المقدرة على الإثبات الجنائي لجرائم نظم المعلومات	2.56	2.00	2.00	.7346	3.00	92.00

جدول رقم (35- أ) يوضح تقييم المهارة العالية لاستخدام الحاسب الآلي والإنترنت

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدودة جداً	2	1.4	5.6	5.6
محدودة	13	9.2	36.1	41.7
متوسطة	10	7.1	27.8	69.4
عالية	8	5.7	22.2	91.7
عالية جداً	3	2.1	8.3	100.0
المجموع	36	25.5	100.0	

جدول رقم (35- ب) يوضح تقييم المعرفة بمتطلبات أمن المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدودة جداً	2	1.4	5.6	5.6
محدودة	24	17.0	66.7	72.2
متوسطة	5	3.5	13.9	86.1
عالية	3	2.1	8.3	94.4
عالية جداً	2	1.4	5.6	100.0
المجموع	36	25.5	100.0	

جدول رقم (35- جـ) يوضح تقييم المقدرة على إتباع السياسة الأمنية للتعامل مع الجرائم

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدودة جداً	1	.7	2.8	2.8
محدودة	6	4.3	16.7	19.4
متوسطة	16	11.3	44.4	63.9
عالية	12	8.5	33.3	97.2
عالية جداً	1	.7	2.8	100.0
المجموع	36	25.5	100.0	

جدول رقم (35- د) يوضح تقييم المعرفة بأساليب ارتكاب جرائم نظم المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدودة جداً	3	2.1	8.3	8.3
محدودة	23	16.3	63.9	72.2
متوسطة	7	5.0	19.4	91.7
عالية	3	2.1	8.3	100.0
المجموع	36	25.5	100.0	

جدول رقم (35- هـ) يوضح تقييم المقدرة على الإثبات الجنائي لجرائم نظم المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
محدودة جداً	1	.7	2.8	2.8
محدودة	18	12.8	50.0	52.8
متوسطة	13	9.2	36.1	88.9
عالية	4	2.8	11.1	100.0
المجموع	36	25.5	100.0	

جدول رقم (36) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم) حيال حجم أسباب الأحجام عن الأبلاغ عن جرائم نظم المعلومات

العنصر	المتوسط	الوسيط	المنوال	الانحراف المعياري	المدى
الحفاظ على السمعة	4.76	5.00	.4294	1.00	495
عدم الرغبة بظهور بمضهر الضحية	4.38	4.00	.6261	2.00	455
الخوف من المسؤولية	4.28	4.00	.7167	2.00	445
محدودية الأثار المترتبة	4.10	4.00	.8535	4.00	426
عدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع	3.62	4.00	1.1174	4.00	376
عدم إبراز كفاءة المجرمين	2.38	2.00	1.2709	3.00	247

جدول رقم (36- أ) يوضح تقييم الحفاظ على السمعة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
عالي	25	17.7	24.0	24.0
عالي جداً	79	56.0	76.0	100.0
المجموع	104	73.8	100.0	

جدول رقم (36- ب) يوضح تقييم عدم الرغبة بظهور بمضهر الضحية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوسط	8	5.7	7.7	7.7
عالي	49	34.8	47.1	54.8
عالي جداً	47	33.3	45.2	100.0
المجموع	104	73.8	100.0	

جدول رقم (36- جـ) يوضح تقييم الخوف من المسؤولية

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوسط	16	11.3	15.4	15.4
عالي	43	30.5	41.3	56.7
عالي جداً	45	31.9	43.3	100.0
المجموع	104	73.8	100.0	

جدول رقم (36- د) يوضح تقييم محدودية الأثار المترتبة

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	3	2.1	2.9	2.9
متوسط	15	10.6	14.4	17.3
عالي	52	36.9	50.0	67.3
عالي جداً	34	24.1	32.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (36- هـ) يوضح التقييم لعدم اكتشاف الجريمة رغم القناعة بإمكانية وجودها في الواقع

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	2	1.4	1.9	1.9
محدود	20	14.2	19.2	21.2
متوسط	20	14.2	19.2	40.4
عالي	36	25.5	34.6	75.0
عالي جداً	26	18.4	25.0	100.0
المجموع	104	73.8	100.0	

جدول رقم (36- و) يوضح التقييم لعدم إبراز كفاءة المجرمين

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
لا يوجد	38	27.0	36.5	36.5
محدود	22	15.6	21.2	57.7
متوسط	11	7.8	10.6	68.3
عالي	33	23.4	31.7	100.0
المجموع	104	73.8	100.0	

جدول رقم (37) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم) حيال مستوى التنسيق بين الجهات الأمنية والمؤسسات المستخدمة للنظم كمعوق من معوقات التحقيق

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوفر وغير مستخدم	3	2.1	2.9	2.9
غير متوفر ولكن ضرورياً	97	68.8	93.3	96.2
ليس ظرورياً	4	2.8	3.8	100.0
المجموع	104	73.8	100.0	

جدول رقم (38) يوضح استجابة عينة الدراسة (المحققين، والعاملين بالنظم) حيال مستوى التنسيق بين المؤسسات المستخدمة لنظم المعلومات والشركات الموفرة لأمن المعلومات

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوفر ومستخدم	22	15.6	21.2	21.2
متوفر وغير مستخدم	66	46.8	63.5	84.6
غير متوفر ولكن ضرورياً	13	9.2	12.5	97.1
ليس ظرورياً	3	2.1	2.9	100.0
المجموع	104	73.8	100.0	

جدول رقم (39) يوضح استجابة عينة الدراسة (المحققين) حيال مدى توفير واستخدام الأجهزة والبرامج المناسبة للتحقيق

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوفرة وغير مستخدمة	5	3.5	13.9	13.9
غير متوفرة ولكن توفرها ضرورياً	31	22.0	86.1	100.0
المجموع	36	25.5	100.0	

جدول رقم (40) يوضح استجابة عينة الدراسة (المحققين) حيال مدى توفير المتخصصين والخبراء في الحاسب الآلي والاستفادة منهم

التقييم	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوفرين ومستفاد منهم	5	3.5	13.9	13.9
متوفرين وغير مستفاد منهم	6	4.3	16.7	30.6
غير متوفرين ولكن توفرهم ضرورياً	25	17.7	69.4	100.0
المجموع	36	25.5	100.0	

جدول رقم (41) يوضح استجابة عينة الدراسة (المحققين) حيال مدى توفرالتدريب في معاهد متخصصة بالتحقيق في جرائم نظم المعلومات

	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
متوفر وغير مستخدم	6	4.3	16.7	16.7
غير متوفر ولكن ضرورياً	30	21.3	83.3	100.0
المجموع	36	25.5	100.0	

جدول رقم (42) يوضح استجابة عينة الدراسة (المحققين) حيال تقييمهم لمدى أهمية أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات

البيان	تسجيل الوقائع	التغير الظاهر على البرامج	وجود أحصنة طروادة	وجود فيروسات
المتوسط	4.5000	3.8611	3.5556	3.5278
الوسيط	5.0000	4.0000	4.0000	4.0000
المنوال	5.00	4.00	4.00	4.00
الانحراف المعياري	.8783	.5426	.9394	.8447
المدى	4.00	3.00	4.00	4.00
المجموع	162.00	139.00	128.00	127.00

جدول رقم (42- أ) يوضح مدى أهمية تسجيل الوقائع كدليل

مدى الأهمية	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم إطلاقاً	1	.7	2.8	2.8
مهم إلى أحد ما	3	2.1	8.3	11.1
مهم	8	5.7	22.2	33.3
مهم جداً	24	17.0	66.7	100.0
المجموع	36	25.5	100.0	

جدول رقم (42- ب) يوضح مدى أهمية التغير الظاهر على البرامج كدليل

مدى الأهمية	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم	2	1.4	5.6	5.6
مهم إلى أحد ما	2	1.4	5.6	11.1
مهم	31	22.0	86.1	97.2
مهم جداً	1	.7	2.8	100.0
المجموع	36	25.5	100.0	

جدول رقم (42- جـ) يوضح مدى أهمية وجود أحصنة طروادة كدليل

مدى الأهمية	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم إطلاقاً	2	1.4	5.6	5.6
غير مهم	4	2.8	11.1	16.7
مهم إلى أحد ما	3	2.1	8.3	25.0
مهم	26	18.4	72.2	97.2
مهم جداً	1	.7	2.8	100.0
المجموع	36	25.5	100.0	

جدول رقم (42-د) يوضح مدى أهمية وجود فيروسات كدليل

مدى الأهمية	التكرار	النسبة	النسبة الحقيقية	النسبة التراكمية
غير مهم إطلاقاً	1	.7	2.8	2.8
غير مهم	4	2.8	11.1	13.9
مهم إلى أحد ما	7	5.0	19.4	33.3
مهم	23	16.3	63.9	97.2
مهم جداً	1	.7	2.8	100.0
المجموع	36	25.5	100.0	

جدول رقم (43) يوضح العلاقات بين التزام المؤسسة بتحديث برامجها وبين حجم حدوث الجرائم التي تتعرض لها

اختبار سبيرمان		تحديث برامج الحماية باستمرار
التلاعب بإدخال البيانات	معامل الارتباط	.118
	الدلالة	.339
تغيير البرامج والإعدادات	معامل الارتباط	.178
	الدلالة	.015
تغيير البيانات بعد إدخالها	معامل الارتباط	.263*
	الدلالة	.030
تدمير الملفات وقواعد البيانات	معامل الارتباط	-.089
	الدلالة	.468
تعطيل المواقع والبرامج والأجهزة	معامل الارتباط	.077
	الدلالة	.535
التنصت والسرقة البيانات	معامل الارتباط	.324**
	الدلالة	.007
نسخ البيانات لاستفادة منها	معامل الارتباط	.289*
	الدلالة	.168
نسخ البرامج والاستخدام غير المصرح به	معامل الارتباط	.385**
	الدلالة	.012
الاستيلاء على ما سوى المعلومات	معامل الارتباط	.037
	الدلالة	.767
إرسال احصنة طروادة	معامل الارتباط	.278*
	الدلالة	.022
إرسال وزراعة فيروسات	معامل الارتباط	.331**
	الدلالة	.006
	العدد	68
الاختراقات البريد الاكتروني	معامل الارتباط	.307*
	الدلالة	.011
	العدد	68
إعتراض الرسائل والتنصت على الشبكات	معامل الارتباط	.157
	الدلالة	.200
إغراق البريد الإلكتروني	معامل الارتباط	.404**
	الدلالة	.064
تحديث برامج الحماية باستمرار	معامل الارتباط	1.000
	الدلالة	.

**. Correlation is significant at the .01 level (2-tailed).

*. Correlation is significant at the .05 level (2-tailed).

جدول رقم (44) يوضح نتائج تحليل التباين لاختلاف رؤية المحققين والعاملين بالنظم

حول أهمية الأدوات المساعدة بضبط في جرائم نظم المعلومات

الأدوات المساعدة بضبط الجريمة	مربع المتوسطات	F	Sig.
سجل الصلاحيات للمستخدمين	.467	9.750	.100
أدوات المراجعة	.662	3.156	.056
أدوات مراقبة المستخدمين للشبكة	1.626	3.745	.078
أدوات التنصت على الشبكة	.369	.759	.470
التقارير التي تنتجها نظم أمن البيانات	7.E-02	.572	.566
مراجعة قاعدة البيانات	7.764	17.68	.000
تقارير الجدران النارية	.507	1.746	.178
برامج تتبع المخترقين	7.360	11.10	.000
برامج تتبع مصدر الرسائل	16.850	25.08	.000
برامج كشف الفيروسات	.121	.626	.536
برامج النسخ الاحتياطي والتسجيل	.182	.985	.376

جدول رقم (44- أ) يوضح نتائج تحليل التباين لاختلاف رؤية المحققين والعاملين بالنظم
حول أهمية الأدوات المساعدة بالضبط والتحقيق في جرائم نظم المعلومات

الأدوات المساعدة بضبط الجريمة	الفرق بين المتوسطات			
	البيان			
	العاملين	المحققين	الموفرين	المعدل
سجل الصلاحيات للمستخدمين	5.0000	4.8056	4.973	4.943
أدوات المراجعة	4.7059	4.8056	4.541	4.688
أدوات مراقبة المستخدمين للشبكة	4.6176	4.6111	4.270	4.525
أدوات التنصت على الشبكة	4.1176	4.2778	4.243	4.191
التقارير التي تنتجها نظم أمن البيانات	4.8824	4.8056	4.865	4.858
مراجعة قاعدة البيانات	3.9265	4.6389	3.811	4.078
تقارير الجدران النارية	4.5441	4.6389	4.405	4.532
برامج تتبع المخترقين	3.8235	4.6111	4.162	4.113
برامج تتبع مصدر الرسائل	3.6176	4.8056	4.162	4.064
برامج كشف الفيروسات	4.7059	4.8056	4.757	4.745
برامج النسخ الاحتياطي والتسجيل	4.7794	4.8056	4.676	4.759

جدول رقم (44- ب) يوضح اختبار شفية لمراجعة قاعدة البيانات

Scheffe

		alpha = .05	
نوع العينة	N	1	2
الموفرين	37	3.8108	
العاملين	68	3.9265	
المحققين	36		4.6389
Sig.		.720	1.000

جدول رقم (44- جـ) يوضح اختبار شفية لبرامج تتبع المخترقين

Scheffe

نوع العينة	N	alpha = .05	
		1	2
العاملين	68	3.8235	
الموفرين	37	4.1622	
المحققين	36		4.6111
Sig.		.159	1.000

جدول رقم (44- د) يوضح اختبار شفية لبرامج تتبع مصدر الرسائل

Scheffe

نوع العينة	N	alpha = .05		
		1	2	3
العاملين	68	3.62		
الموفرين	37		4.1622	
المحققين	36			4.806
Sig.		1.000	1.000	1.000

جدول رقم (45) يوضح نتائج تحليل التباين في رؤية المحققين والعاملين بالنظم وموفري التقنيات حول أهمية الأدوات المساعدة بالتحقيق في جرائم نظم المعلومات

الأدوات المساعدة بالتحقيق	متوسط المربعات	F	Sig.
أداة فك التشفير	19.204	27.227	.000
برامج كسر كلمة المرور	1.492	1.641	.198
أدوات استرجاع المعلومات من الأقراص	19.865	26.769	.000
برامج الضغط وفك الضغط	2.265	4.090	.019
برامج البحث عن الملفات العادية والمخفية	16.716	39.927	.000
برامج اتصالات	44.725	128.645	.000
برامج تشغيل الحاسب	.528	1.999	.139
برامج نسخ البيانات	.320	1.004	.369
برامج مقارنة النسخ	19.656	41.813	.000

جدول رقم (45 - أ) يوضح الاختلاف في رؤية المحققين والعاملين بالنظم وموفري التقنيات حول أهمية الأدوات المساعدة بالتحقيق في جرائم نظم المعلومات

الأدوات المساعدة بالتحقيق	الفرق بين المتوسطات			
	البيان			
	العاملين	المحققين	الموفرين	المعدل
أداة فك التشفير	3.529	4.8056	3.9189	3.9574
برامج كسر كلمة المرور	3.794	4.0000	4.1351	3.9362
أدوات استرجاع المعلومات الأقراص التالفة	3.721	4.8056	3.4324	3.9220
برامج الضغط وفك الضغط	3.088	3.1944	2.7297	3.0213
برامج البحث عن الملفات العادية والمخفية	2.824	4.0000	3.0541	3.1844
برامج اتصالات	1.877	3.8333	2.4054	2.5290
برامج نسخ البيانات	3.015	3.0000	3.1622	3.0496
برامج مقارنة النسخ	3.559	4.6667	3.3243	3.7801

جدول رقم (45- ب) يوضح اختبار شفية لأداة فك التشفير

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	3.5294	
الموفرين	37	3.9189	
المحققين	36		4.8056
Sig.		.102	1.000

جدول رقم (45- جـ) يوضح اختبار شفية لأدوات استرجاع المعلومات من الأقراص التالفة

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
الموفرين	37	3.4324	
العاملين	68	3.7206	
المحققين	36		4.8056
Sig.		.302	1.000

جدول رقم (45- د) يوضح اختبار شفية لبرامج الضغط وفك الضغط Pkzip

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
الموفرين	37	2.7297	
العاملين	68	3.0882	3.0882
المحققين	36		3.1944
Sig.		.085	.803

جدول رقم (45- هـ) يوضح اختبار شفية لبرامج البحث عن الملفات العادية والمخفية

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	2.8235	
الموفرين	37	3.0541	
المحققين	36		4.0000
Sig.		.258	1.000

جدول رقم (45- و) يوضح اختبار شفية لبرامج اتصالات مثل Lantastic

Scheffe

نوع العينة	العدد	Subset for alpha = .05		
		1	2	3
العاملين	65	1.8769		
الموفرين	37		2.4054	
المحققين	36			3.8333
Sig.		1.000	1.000	1.000

جدول رقم (46) يوضح اختبار (بيرسون كاي تربيع) للفرق بين رؤية العاملين بالنظم والمحققين نحو وسائل التعرف على شخصية مرتكب الجريمة

البيان	القيمة	درجة الحرية	Sig.
قيمة بيرسون كاي تربيع	30.601	4	.000
النسبة المرجحة	37.891	4	.000
الاتصال الخطي	25.022	1	.000
العدد	104		

جدول رقم (46- أ) يوضح الفروق في رؤية المحققين والعاملين بالنظم نحو وسيلة التعرف على شخصية مرتكب جريمة نظم المعلومات

Count

وسيلة التعرف على شخصية مرتكب جريمة نظم المعلومات	نوع العينة	
	العاملين	المحققين
عنوان IP	.0	5.6
برامج الحماية	.0	8.3
وسائل تتبع المخترقين	.0	5.6
برامج تتبع مصدر الرسائل	.0	5.6
عنوانIP +برامج الحماية	27.9	5.6
عنوانIP +وسائل تتبع المخترقين +برامج الحماية	58.8	55.6
+ برامج الحماية + تتبع المخترقين +تتبع مصدر الرسائل عنوانIP	13.2	13.89
المجموع	100.0	100.0

جدول رقم (46- ب) يوضح الفروق في رؤية المحققين والعاملين بالنظم نحو إلى أي مدى يمكن الاستفادة من الوسيلة بتعرف على شخصية مرتكب جريمة نظم المعلومات

Count

وسيلة التعرف على شخصية مرتكب جريمة نظم المعلومات	نوع العينة	
	العاملين	المحققين
عنوان IP	100.0	80.7
برامج الحماية	100.0	69.5
وسائل تتبع المخترقين	58.8	22.5
برامج تتبع مصدر الرسائل	13.2	19.5

جدول رقم (47) يوضح اختبار (بيرسون كاي تربيع) للفرق بين رؤية العاملين بالنظم والمحققين نحو مساعدة برامج الحماية بضبط جريمة نظم المعلومات

البيان	القيمة	درجة الحرية	Sig.
قيمة بيرسون كاي تربيع	25.413	6	.000
النسبة المرجحة	34.082	6	.000
الاتصال الخطي	15.868	1	.000
العدد	104		

جدول رقم (47- أ) يوضح الفروق في رؤية المحققين والعاملين بالنظم نحو مساعدة برامج الحماية بضبط جريمة نظم المعلومات

Count

تساعد برامج الحماية في	نوع العينة	
	العاملين	المحققين
تحديد نوع الجريمة المرتكبة	.0	2.8
تحديد توقيت ارتكابب الجريمة	.0	5.6
تحديد مصدر الجريمة	.0	8.3
الإعلام بوجود جريمة مرتكبة	.0	2.8
تحديد نوع الجريمة وتوقيت ارتكابها	7.4	.0
تحديد نوع الجريمة وتوقيت ارتكابها والإعلام بوجودها	25.0	.0
تحديد نوعها ومصدرها وتوقيت ارتكابها والإعلام بوجودها	67.6	80.6

جدول رقم (47- ب) يوضح الفروق في رؤية المحققين والعاملين بالنظم نحو إلى أي مدى يمكن الاستفادة من مساعدة برامج الحماية بضبط جريمة نظم المعلومات

Count

العنصر	نوع العينة	
	العاملين	المحققين
تحديد نوع الجريمة المرتكبة	100.0	83.4
تحديد توقيت ارتكاب الجريمة	100.0	86.2
تحديد مصدر الجريمة	67.6	80.6
الإعلام بوجود جريمة مرتكبة	92.6	80.6

جدول رقم (48) يوضح نتائج تحليل التباين في رؤية المحققين والعاملين بالنظم وموفري التقنيات حول أهمية الأدوات المساعدة بالتحقيق في جرائم نظم المعلومات

المعوق	مجموع المربعات	درجة الحرية	متوسط المربعات	F	Sig.
عدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد	1.661	2	.831	2.538	.083
مكونات عناصر جريمة نظم المعلومات غير	2.598	2	1.299	4.061	.019
عدم وجود قسم متخصص في جرائم المعلوماتية	118.393	2	59.20	178	.000
عدم وجود متابعة للمستجدات حول جرائم نظم	1.52E-02	2	.008	.024	.977
عدم وجود مردود مادي ملحوظ لتحديث برامج	6.059	2	3.029	3.202	.044
عدم قناعة لدى العاملين في مجال نظم	58.039	2	29.02	20.4	.000
معظم المؤسسات المتضررة من جرائم نظم	6.359	2	3.180	4.541	.012
مقاومة الموظفين الوسائل الأمنية للإبقاء على	5.977	2	2.988	7.373	.001
عدم استخدام أدوات تقنية متطورة تناسب برامج	22.785	2	11.39	40.9	.000
عدم التدريب على استخدام التقنية المساعدة	39.420	2	19.71	58.6	.000
عدم الاستعانة بخبراء وباستشاريين في مجال	194.550	2	97.27	137	.000
تصميم البرامج بطريقة لا تسمح لها بالعمل مع	11.762	2	5.881	6.809	.002
إمكانية ارتكاب هذه الجرائم عن بعد باستخدام	15.211	2	7.605	14.7	.000

جدول رقم (48- أ) يوضح نتائج تحليل التباين في رؤية المحققين والعاملين بالنظم وموفري التقنيات نحو معوقات استخدام وسائل التحقيق في جرائم نظم المعلومات

المعوق	الفرق بين المتوسطات			
	البيان			
	العاملين	المحققين	الموفرين	المجموع
عدم وجود تشريعات واضحة خاصة بجرائم نظم المعلومات في البلد	4.6029	4.8056	4.5135	4.6312
مكونات عناصر جريمة نظم المعلومات غير معروفة للأطراف المعنية بالجريمة	3.6618	3.3333	3.5946	3.5603
عدم وجود قسم متخصص في جرائم المعلوماتية	2.4265	4.4444	2.2162	2.8865
عدم متابعة للمستجدات حول جرائم نظم المعلومات	2.9412	2.9444	2.9189	2.9362
عدم وجود مردود مادي ملحوظ لتحديث برامج الحماية والتحقيق	3.0735	2.8333	3.4054	3.0993
عدم قناعة العاملين في مجال نظم المعلومات بتدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية	2.4853	4.0556	3.0270	3.0284
معظم المؤسسات المتضررة من جرائم نظم المعلومات لا تتقدم بشكوى للجهات الرسمية	4.1324	4.3333	3.7568	4.0851
مقاومة الموظفين الوسائل الأمنية للإبقاء على قدر من الحرية	3.7647	4.1667	3.6216	3.8298
عدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق	3.2206	4.1667	3.2973	3.4823
عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين	3.5000	4.7500	3.6216	3.8511
لا تتم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات	2.0294	4.7500	2.1081	2.7447
تصمم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية	1.9265	2.6111	2.0000	2.1206
إمكانية ارتكاب هذه الجرائم عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط	1.7059	2.5000	1.8649	1.9504

جدول رقم (48- ب) يوضح اختبار شفية لمكونات عناصر جريمة نظم المعلومات غير معروفة للأطراف المعنية بالجريمة

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
المحققين	36	3.3333	
الموفرين	37	3.5946	3.5946
العاملين	68		3.6618
Sig.		.104	.859

جدول رقم (48- جـ) يوضح اختبار شفية لعدم وجود قسم متخصص في جرائم المعلوماتية

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
الموفرين	37	2.2162	
العاملين	68	2.4265	
المحققين	36		4.4444
Sig.		.241	1.000

جدول رقم (48- د) يوضح اختبار شفية لمعوق عدم استطاعة المؤسسات استخدام وسائل التحقيق بسبب التكلفة المالية المرتفعة

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
المحققين	36	2.0000	
الموفرين	37		3.6216
العاملين	68		4.0294
Sig.		1.000	.312

جدول رقم (48- هـ) يوضح اختبار شفية لمعوق عدم وجود مردود مادي ملحوظ لتحديث برامج الحماية والتحقيق

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
المحققين	36	2.8333	
العاملين	68	3.0735	3.0735
الموفرين	37		3.4054
Sig.		.519	.288

جدول رقم (48- و) يوضح اختبار شفية لمعوق عدم قناعة لدى العاملين في مجال نظم المعلومات بتدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	2.4853	
الموفرين	37	3.0270	
المحققين	36		4.0556
Sig.		.111	1.000

جدول رقم (48- ز) يوضح اختبار شفية لمعوق المؤسسات المتضررة من جرائم نظم المعلومات لا تتقدم بشكوى للجهات الرسمية

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
الموفرين	37	3.7568	
العاملين	68	4.1324	4.1324
المحققين	36		4.3333
Sig.		.118	.538

جدول رقم (48- ح) يوضح اختبار شفية لمعوق مقاومة الموظفين للوسائل الأمنية للإبقاء على قدر من الحرية

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
الموفرين	37	3.6216	
العاملين	68	3.7647	
المحققين	36		4.1667
Sig.		.581	1.000

جدول رقم (48- ط) يوضح اختبار شفية لعدم استخدام أدوات تقنية متطورة تناسب برامج وأدوات التحقيق

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	3.2206	
الموفرين	37	3.2973	
المحققين	36		4.1667
Sig.		.796	1.000

جدول رقم (48- ي) يوضح اختبار شفية لمعوق عدم التدريب على استخدام التقنية المساعدة في كشف المجرمين

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	3.5000	
الموفرين	37	3.6216	
المحققين	36		4.7500
Sig.		.623	1.000

جدول رقم (48- ك) يوضح اختبار شفية لمعوق عدم الاستعانة بخبراء وباستشاريين في مجال أمن نظم المعلومات

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	2.0294	
الموفرين	37	2.1081	
المحققين	36		4.7500
Sig.		.910	1.000

جدول رقم (48- ك) يوضح اختبار شفية لمعوق تصميم البرامج بطريقة لا تسمح لها بالعمل مع أدوات تحقيق خارجية

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	1.9265	
الموفرين	37	2.0000	
المحققين	36		2.6111
Sig.		.935	1.000

جدول رقم (48- ل) يوضح اختبار شفية لإمكانية ارتكاب هذه الجرائم عن بعد باستخدام شبكة الإنترنت بينما الأدوات تعمل في بيئة محلية فقط

Scheffe

نوع العينة	العدد	alpha = .05	
		1	2
العاملين	68	1.7059	
الموفرين	37	1.8649	
المحققين	36		2.5000
Sig.		.592	1.000