DOI: 10.32347/2412-9933.2020.42.56-62
УДК 004.415.53

Криворучко Олена Володимирівна
Доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки, *orcid.org/0000-0002-7661-9227*
Київський національний торговельно-економічний університет, Київ
Сунічук Олена Миколаївна
Директор, *orcid.org/0000-0002-6775-7222*
ТОВ «Новелл Консалтинг», Київ
Швець Денис Валеріянович
Керівник відділу аудиту ІТ та ІБ, *orcid.org/0000-0002-7661-9227*
ТОВ «Новелл Консалтинг», Київ
Мінін Олександр Володимирович
Інженер засобів безпеки відділу з аудиту інформаційної безпеки, *orcid.org/0000-0002-2288-8640*
ТОВ Новелл Консалтинг, Київ

АНАЛІЗ СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Анотація. *В час постійної інформатизації суспільства, стрімкого розвитку інформаційних технологій, збільшення кількості нових програмних продуктів та відповідно інформаційних систем гостро стоїть питання захисту від несанкціонованих вторгнень в інформаційні системи та захисту даних. Визначено що IT-аудит є ключовим компонентом досягнення якісної роботи інформаційної системи, що гостро відображає проблему підготовки фахівців, які не в змозі ефективно, коректно та швидко підтримувати роботу інформаційної системи від спотворень зловмисників та дані в безпеці. Проаналізовано динаміку кібератак на інформаційні ресурси нашої держави та правову складову кіберзахисту України. Проблема захисту стоїть гостро і піднімається дуже вузьким колом науковців. Але підґрунтя розвитку та впровадження IT-аудиту закладено. Відповідно до правового поля України спеціальні державні установи не лише встановлюють вимоги щодо захисту інформації, але і проводять перевірки стану захищеності систем. Розгляд міжнародного стандарту ISO / IEC 27001:2013 дає можливість побачити яким чином система стандартів працює на підтримку інформаційних систем в сегменті інформаційної безпеки, яким чином підприємство/організація будь-якої форми власності матиме якісний алгоритм захисту інформації і яким чином проводиться IT-аудит інформаційних систем. ISO / IEC 27001:2013 надає низку перспектив для управління інформаційною безпекою підприємства/організації – виявляє ризики та застосовує засоби контролю для управління або уникнення інформаційних загроз; підсилює гнучкість в адаптації управління до всіх або окремих підсистем діяльності підприємства/організації; дає можливість отримати зацікавленість та довіру клієнтів, що її дані захищені; показує сучасність та надійність захисту інформаційної системи. Саме система міжнародних стандартів та приклади таких організацій, як глобальна асоціація ISACA логічно підводять до висновку, що проведення IT-аудиту є необхідним для керування інформаційними системами. Гостро постає питання у підготовці IT-аудиторів, які мають бути сертифікованими та відповідати світовим стандартам.*

Ключові слова: інформацій система; інформаційна безпека; концепція безпеки; політика інформаційної безпеки; загрози; комп'ютерна система; кібераудит; ІКТ; захист інформації; кіберзагрози

Вступ

В умовах стрімкого розвитку інфраструктури та поглиблення інформатизації соціально-економічних процесів ефективність діяльності підприємств, установ та організацій будь-якої форми власності дедалі більше залежить від інформаційних технологій (ІТ), що використовуються в системах управління.

На сьогодні середовище інформаційних технологій (ІТ-середовище) як структурна складова організації є досить складною системою, яка об'єднує різноманітні інформаційні, програмні, апаратні засоби та безумовно людські ресурси для досягнення ефективної роботи організації, підприємства, установи. Всі поставленні завдання формують потребу у підвищенні ефективності й економічності

використання ІТ, збільшення переваг і усунення недоліків від їх застосування, а також обґрунтування витрат на ІТ. Для втілення в виробничі процеси такої потреби все більшого значення набуває постійне застосування в системі управління організацій аудиту інформаційних технологій (ІТ-аудиту).

ІТ-аудит є ключовим компонентом для забезпечення якості інформаційних систем та прикладного програмного забезпечення. Без надійних інформаційних систем та результативних ІТ-заходів контролю організація не в змозі правильно виконувати операції/транзакції та узагальнювати надійну фінансову звітність, що, своєю чергою, впливає на рівень досягнення поставлених перед нею завдань і цілей.

Постановка проблеми

Протягом останніх років не лише пересічні громадяни України, а й державні установи зазнали суттєвих втрат інформаційних ресурсів через здійснення кібератак. Перша зареєстрована успішна кібератака на енергетичну систему України з виведенням її з ладу сталася 23 грудня 2015 року. Російським зловмисникам вдалося успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній.

В Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII визначено, що

«Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що опрацьовуються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [1].

Як відомо 6 грудня 2016 р. була здійснена хакерська атака на урядові інформаційно-телекомунікаційні системи, серед яких Міністерство фінансів України, Державна казначейська служба. Вона призвела до масштабних затримок бюджетних виплат [2].

Відповідно до заяви Казначейства щодо вчинення атаки було проведено розслідування Департаменту кіберполіції Національної поліції України. Керуючись зробленими висновками розслідування цієї події, встановлено передумови та причини кібератаки, серед яких є факти використання в органах Казначейства застарілого комп'ютерного обладнання та операційних систем, які не підтримуються вітчизняним виробником, відсутність постійного та відповідного рівня фінансування на оновлення комп'ютерного, серверного обладнання, операційних систем, побудови систем аналізу та виявлення шкідливого програмного забезпечення, систем керування інформаційною безпекою, запровадження технічних рішень щодо створення захищеного інформаційного середовища в органах Казначейства усіх рівнів.

Спеціалізовані перевірки захищеності інформаційних ресурсів в Україні здійснює Державна служба спеціального зв'язку та захисту інформації України. Проте цією службою охоплюється лише технічна сторона питання. Управлінська та фінансова складові рішень керівництва щодо забезпечення належного функціонування інформаційних систем, моніторинг та аналіз систем внутрішнього контролю і досі не є об'єктом зовнішніх перевірок з боку органів державного контролю.

Події кінця 2016 року засвідчили вразливість і відкритість урядових установ для кібератак через відсутність контрольованості трьох основних заходів безпеки, таких як: технічне обмеження на програми завантаження, обмежене використання прав локальних адміністраторів, систематичні оновлення програмного забезпечення [3].

Ці заходи безпеки ІТ-систем мають бути предметом першочергової уваги під час управління стратегічно важливими установами державного сектору, що актуалізує дослідження з цього питання.

Системний та постійний характер впливу на інформаційну безпеку великої сукупності різних обставини, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, призводять до необхідності комплексного підходу при вирішенні проблеми безпеки інформаційних систем та мінімізації уникнення кібератак [4].

Аналіз останніх досліджень і публікацій

Аудит ефективності та безпеки ІТ-систем установ державного сектору економіки лише в окремих аспектах теоретичних і практичних розробок досліджувався зарубіжними та вітчизняними вченими. Особливості аудиту інформаційних технологій було започатковано С.В. Івахненковим. Проте він розглядав переважно методику та організацію аудиту в умовах інформаційних систем реального сектору економіки.

Серед праць, які присвячені дослідженням методологічних, сутнісних та змістовних основ безпеки ІТ-систем особливе місце посідають теоретичні розроблення Е. Бєляєва, М. Бусленка, С. Гриняєва, О. Данильяна, О. Дзьобаня, Г. Ємельянова, В. Лопатіна, О. Позднякова, Л. Сергієнка, В. Циганкова, М. Чеснокова та інших дослідників. Авторами робіт, у яких розкриваються особливості забезпечення інформаційної безпеки, є О. Дзьобаня, А. Колодюк, В. Копилов, А. Кубишкін, Є. Мануйлов, В. Ніцевич, А. Стрельцов, М. Якушев та ін.

Дослідження перелічених учених дозволили сформувати у вітчизняній теорії понятійний апарат ІТ-аудиту.

Виклад основного матеріалу

Нині основними документами, які регулюють питання, пов'язані із захистом інформації в інформаційно-телекомунікаційних системах, є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (від 05.07.1994) та «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». (Постанова Кабінету Міністрів України від 29.03.2006 р. № 373). Згідно даних нормативних документів, основною вимогою до інформаційних систем з точки зору безпеки – є наявність в них побудованої комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. При цьому необхідність побудови КСЗІ визначається типом інформації, що працює в цій системі. Такими видами є секретна інформація, службова інформація, конфіденційна інформація (наприклад, персональні дані) та державні інформаційні ресурси. Порядок побудови та вимоги до цих систем визначаються нормативними документами системи технічного захисту інформації (НД ТЗІ). Згідно із законом «Про Державну службу спеціального зв'язку та захисту інформації України» (Закон України» № 3475-IV від 23.02.2006 № 2163-VIII від 05.10.2017, *ВВР*, 2017, № 45, ст.403), головним регулятором в області інформаційної безпеки є Державна служба спеціального зв'язку та захисту інформації України. Згідно даного нормативного акту служба не тільки встановлює вимоги щодо захисту інформації, але і проводить перевірки стану захищеності систем. Свою діяльність з перевірок захисту інформації в комп'ютерних системах державний регулятор здійснює на підставі наказу «Про затвердження Положення про державний контроль за станом ТЗІ» (Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87), наказу «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах» (Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660) [5]. Для попередження і мінімізації деструктивного впливу кіберзагроз створюються відповідні системи захисту. Проте виникає проблема оцінки того, наскільки якісно система захисту може протидіяти загрозам. Відповідно система захисту несанкціонованих доступів до ІТ-системи вимагає професійно-сформованої команди. Підготовка такого плану фахівців має відповідати передусім вимогам ISO 19011 (Стандарт ISO 19011:2018), який розроблено Технічним комітетом ТК 176 Міжнародної організації по стандартизації ISO. Стандарт ISO 19011:2018 можуть застосовувати широкі кола потенційних користувачів, включаючи аудиторів, організації, які впроваджують системи менеджменту, і організації, яким необхідно проводити аудити систем менеджменту відповідно до контракту або законодавства. Проведення аудиту відповідно до стандарту засноване на менеджменті ризиків і передбачає застосування вибіркових досліджень на основі теорії ймовірностей і математичній статистиці.

Фахівці з боротьби з кіберзагрозами мають бути постійно обізнані в розвитку ІТ-новинок і ризиків, які можуть виникнути під час несанкціонованих вторгнень в систему. Фахівці, які можуть проводити ІТ-аудит або ж аудит інформаційних систем та їх безпеки, повинні бути в змозі визначити та оцінити ризики, які притаманні конкретній організації, а також допомогти їй у досягненні бізнес-цілей розробивши, впровадивши та провівши моніторинг дієвих і ефективних контролів інформаційних систем, які засновані на оцінці ризиків – зазначав Урс Фішер, голова робочої групи ISACA з сертифікації CRISC. В ІТ секторі існує прогалина з фахівцями кіберпростору, а саме фахівцями з кібераудиту. Забезпечити скоординовані дії керівництва та співробітників організації в разі вторгнення зловмисників в комп'ютерні системи, знизити негативні наслідки інциденту, провести стримування зловмисників та їх викорінення із ІТ систем організації – це і є головне завдання проведення ІТ-аудиту інформаційних систем. Завдання будь-якої організації уникнути заздалегідь кіберінцидентів.

Впровадження ISO / IEC 27001:2013 надає низку перспектив для управління інформаційною безпекою підприємства/організації будь-якої форми власності, а саме:

– виявити ризики та застосувати засоби контролю для управління або уникнення інформаційних загроз;

– надає гнучкість в адаптації управління до всіх або окремих сегментів діяльності підприємства/організації;

– дає можливість отримати зацікавленість та довіру клієнтів, що їх дані захищені;

– задовольнити такі надії, демонструючи відповідність часу.

Система управління інформаційною безпекою ISO / IEC 27001:2013 допомагає впровадити найкращу практику для покращення захисту даних та усунення загрози порушення безпеки інформаційних систем. А ефективне управління безпекою інформаційних систем підтримується при регулярному моніторингу або аудиті системи. Щоб робити це якісно, поглиблене розуміння серії ISO 27k дають змогу взяти на себе відповідальність головного аудитора. Сертифікація третьої сторони – органу оцінки відповідності дає додаткову впевненість ключовим зацікавленим сторонам у тому, що ризики безпеки інформаційних систем ефективно управляються. Щороку витрачається понад 1 мільйон годин, щоб покращити ефективність бізнесу в усьому світі в сегменті безпеки інформаційних систем.

Кібераудити мають вирішальне значення для постійного вдосконалення системи управління інформаційною безпекою ISO / IEC 27001. У міру розвитку технологій повинні захищатися дані для підтримки відповідності ISO / IEC 27001. Незалежні та сторонні аудити дають змогу експертам оцінити всі процеси та засоби захисту інформації в інформаційних системах. А їх результати допоможуть виявити наявні або потенційні загрози для цих фізичних осіб чи компаній/організацій, допомагаючи тим самим постійно вдосконалювати спосіб управління інформаційною безпекою.

Знання ISO / IEC 27001 допоможе зрозуміти вимоги стандарту з точки зору аудитора. Важливо вміти планувати, проводити та звітувати про аудит, вдосконалюючи методи інтерв'ю, переглядаючи загрози та вразливості безпеці, а також визначаючи правильні елементи управління ними.

Таблиця – ***Вплив ISO / IEC 27001:2013 на роботу компанії/організації***

Сфери прояву бізнесу	**Як допомагає ISO / IEC 27001:2013**	**Користь для підприємства/організації**
Репутація	Допомагає визначити ризики для інформації та вживати заходів щодо управління чи зменшення їх	Підвищення репутації та довіри зацікавлених сторін
	Допомагає встановити процедури для швидкого виявлення порушень інформаційної безпеки	Прозорість видимості ризику серед зацікавлених сторін
	Вимагає від керівництва постійно вдосконалювати систему управління інформаційною безпекою (isms)	Вибудовує довіру та надійність на ринку/ в суспільстві
Зацікавлені сторони	Вимагає визначити всіх внутрішніх та зовнішніх зацікавлених сторін, яких стосуються isms	Поліпшення поінформованості щодо інформаційної безпеки серед усіх відповідних сторін
	Вимагає від вас повідомляти політику isms та гарантувати, що персонал розуміє, як вони цьому сприяють	Зменшує ймовірність порушень інформаційної безпеки, пов’язаних із персоналом
	Вищому керівництву необхідно визначити ролі isms та забезпечити, щоб люди були компетентними	Виявляє прихильність до інформаційної безпеки на всіх рівнях роботи підприємства/організації
Відповідності	Надає основу, яка допомагає вам керувати своїми юридичними та нормативними вимогами	Знижує ймовірність штрафу чи притягнення до відповідальності
	Змушує переглядати та повідомляти свої регулярні вимоги іншим зацікавленим сторонам	Допомагає виконувати відповідне законодавство та допомагає бути в курсі останніх
Ризик управління	Змушує оцінювати ризики для інформаційної безпеки, щоб була можливість виявити потенційні недоліки та реагувати	Допомагає захистити інформацію, та тим самим забезпечує безперебійну роботу і мінімізує збої
	Вимагає встановити контроль, пропорційний ризикам	Економить витрати за рахунок мінімізації інцидентів
	Спонукає постійно оцінювати ризики інформаційної безпеки та переконуватись, що введений контроль є відповідним	Забезпечує захист, доступність інформації та доступ до неї

Висновки

Підготовка фахівців для національної системи кібербезпеки має бути керована та контрольована, а також має ґрунтуватись на компетентностях здобутих як на основі теоретичних знань, так і практичних навичок.

Інформаційні системи державних установ, організацій та підприємств потребують уваги з точки зору забезпечення кібербезпеки. Щодо аудиту безпеки інформаційних систем доцільно керуватися міжнародними стандартами та досвідом міжнародних організацій та систем сертифікації.

Розуміння сфери застосування стандарту ISO / IEC 27001 впливає на процес управління компанією/організацією та даними про клієнтів, працюючи на якісний показник. Проводячи аудит системи управління інформаційною безпекою, інформаційна система буде надійною системою захисту даних. Також це допоможе створити культуру поінформованості про безпеку у своїй організації, підтримуючи відповідність ISO / IEC 27001, зміцнюючи довіру клієнтів до здатності захищати їх дані.

Список літератури

1. *Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Електронний ресурс. Точка доступу: https://zakon.rada.gov.ua/laws/show/2163-19*
2. *Порталт газети «Українська правда». Електронний ресурс. Точка доступу: https://www.epravda.com.ua/publications/2016/12/9/613957/*
3. *Портал «Держкомзв'язок». Шляхи вирішення проблеми інформаційної безпеки в Україні. Електронний ресурс. Точка доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=CE0C98AFB4AE2CF71790756873D292F6?art_id=38826&cat_id=38712*
4. *Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту // Ефективна економіка. – № 5, 2020.*
5. *Кальченко В.В. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем // Системи управління, навігації та зв'язку. –2018. – №4. – С. 109 – 114.*
6. *Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. – М.: МГИУ, 2005. – 215 с.*
7. *Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.*
8. *Конев И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.*
9. *Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.*
10. *Аникин И.В., Глова В.И., Нейман Л.И., Нигматуллина А.Н. Теория информационной безопасности и методология защиты информации // Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008 с. 358.*
11. *Сороковская А.А. Информационная безопасность предприятия: новые угрозы и перспективы [Электронный ресурс]. – Режим доступа: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.*
12. *Курушин В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. – М.: Новый юрист. – 2012. – 256 с.*
13. *Гатчин Ю.А. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В.В. Сухостат. – СПб.: СПбГУ ИТМО, 2010. – 98 с.*
14. *Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.*
15. *Дронь М.М., Малайчук В.П., Петренко О.М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.*
16. *Даник Ю.Г., Супрунов Ю.М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України. Збірник наукових праць ЖВІ НАУ "Інформаційні системи", 2011. – С. 5 – 22.*
17. *Міночкін А.І. Інформаційна боротьба: сучасний стан та досвід підготовки фахівців // Оборонний вісник. – К.: Центр воєнної політики та політики безпеки, 2011. – №2. – С. 12 – 14.*
18. *Сисоєв В. Аналіз рівня освіти та підготовки фахівців з управління IT та інформаційної безпеки в Україні. [Електронний ресурс]. – Режим доступу: http://www.auditagency.com.ua/blog/ISACA_research_Education.pdf. Дата звернення: 24 травня 2018.*
19. *Перший стандарт вищої освіти стосується кібербезпеки. [Електронний ресурс]. Режим доступу: https://ligazakon.net/lawnews/doc/-nz173112-pershyy-standart-vyshchoyi-osvity-stosuyetsya-kiberbezpeky?type=ep. Дата звернення: 24 травня 2018.*
20. *Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners/NATO Members, 4500-1 (OSEM PED)", Oct. 2016, 73 p.*
21. *"ISO/IEC 27032:2012. Information technology. – Security techniques. – Guidelines for cybersecurity", 50 p.*
22. *Center for Internet Security, CIS Controls Version 7 – What's Old, What's New [Електронний ресурс]. Режим доступу: https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/. Дата звернення: 24 травня, 2019.*
23. *Center for Internet Security. CIS Controls [Електронний ресурс]. Режим доступу: https://www.cisecurity.org/controls/. Дата звернення: 24 травня, 2019.*

Стаття надійшла до редколегії 03.04.2020

Криворучко Елена Владимировна
Доктор технических наук, профессор, заведующий кафедрой инженерии программного обеспечения кибербезопасности, *orcid.org/0000-0002-7661-9227*
Киевский национальный торгово-экономический университет, Киев
Суничук Елена Николаевна
Директор, *orcid.org/0000-0002-6775-7222*
ООО "Новелл Консалтинг", Киев
Швец Денис Валериянович
Начальник отдела аудита информационной безопасности, *orcid.org/0000-0002-5460-856X*
ООО "Новелл Консалтинг", Киев
Минин Александр Владимирович
Инженер систем безопасности отдела аудита информационной безопасности, *orcid.org/0000-0002-2288-8640*
ООО "Новелл Консалтинг", Киев

АНАЛИЗ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Аннотация. *Во время постоянного повышения информатизации общества, стремительного развития информационных технологий, увеличения количества новых программных продуктов и соответственно информационных систем остро стоит вопрос защиты от несанкционированных вторжений в информационные системы и защиты данных. Установлено, что ИТ-аудит является ключевым компонентом достижения качественной работы информационной системы. Кроме того, остро стоит проблема с наличием специалистов, которые в состоянии эффективно, корректно и быстро поддерживать работу информационной системы, защищая ее от злоумышленников и сберегая данные в безопасности. Проанализирована динамика кибератак на информационные ресурсы нашего государства и правовую составляющую киберзащиты Украины. Проблема защиты стоит остро, но поднимается очень узким кругом ученых. Но основы развития и внедрения ИТ-аудита заложены. В соответствии с правовым полем Украины специальные государственные учреждения не только устанавливают требования по защите информации, но и проводят проверки состояния защищенности систем. Рассмотрение международного стандарта ISO / IEC 27001 дает возможность увидеть, каким образом система стандартов работает в поддержку информационных систем в сегменте информационной безопасности, каким образом предприятие / организация любой формы собственности будет обеспечивать качественный алгоритм защиты информации и каким образом проводится ИТ-аудит информационных систем. ISO / IEC 27001 предоставляет ряд перспектив для управления информационной безопасностью предприятия / организации – обнаруживает риски и применяет средства контроля для управления или предотвращения информационных угроз; усиливает гибкость адаптации управления ко всей или отдельным подсистемам деятельности предприятия / организации; дает возможность получить заинтересованность и доверие клиентов, данные которых защищены; показывает современность и надежность защиты информационной системы. Именно система международных стандартов и примеры таких компаний, как группы ISACA логически подводят к выводу, что проведение ИТ-аудита необходимо для управления информационными системами. Также стоит отметить, что остро стоит вопрос в подготовке ИТ аудиторов, которые должны быть сертифицированы и соответствовать мировым стандартам.*

Ключевые слова: информационная система; информационная безопасность; концепция безопасности; политика информационной безопасности; угрозы; компьютерная система; кибераудит; защита информации; киберугрозы

Kryvoruchko Olena
DSc (Eng.), Professor, Head of the Department of at Software Engineering and Cyber Security, *orcid.org/0000-0002-7661-9227*
Kyiv National University of Trade and Economics, Ukraine
Synichuk Olena
Director, orcid.org, *orcid.org/0000-0002-6775-7222*
Novell Consulting, LLC, Ukraine
Shvets Denys
Head of the Information Security Audit Department, *orcid.org/0000-0002-5460-856X*
Novell Consulting LLC, Ukraine
Olexander Minin
Security engineer of the Information Security Audit Department, *orcid.org/0000-0002-2288-8640*
Novell Consulting LLC, Ukraine

ANALYSIS OF THE SECURITY STATUS OF INFORMATION AND TELECOMMUNICATION SYSTEMS

Abstract*. At a time society constant informatization, the rapid information technology development, increasing the number of new software products and information systems, the question of protection against unauthorized intrusions into information systems and data protection is acute. It is determined that IT audit is a key component of achieving quality work of the information system and a problem with professionals who are able to effectively, correctly and quickly support the information system from malformations and data security. The dynamics of cyberattacks on state information resources and the legal component of Ukraine cyber defense are analyzed. The problem of protection is raised by a very narrow circle of scientists. But the foundation for the development and implementation of IT audit is laid. In accordance with the legal field of Ukraine, special state institutions not only establish requirements for the information protection, but also conduct inspections of the systems security. Consideration of the international standard ISO / IEC 27001 gives an opportunity to see how the standards system works to support security of*

information systems, how an enterprise / organization of any ownership form will have a quality information protection algorithm and how IT audit of information systems. ISO / IEC 27001 provides a number of perspectives for the management of the enterprise / organization information security – identifies risks and applies controls to managing or avoiding of information threats; enhances flexibility in the adaptation management to all or some subsystems of the enterprise / organization; provides an opportunity to gain the customers interest and trust that their data is protected; shows the modernity and reliability of information system protection. It is the system of international standards and examples of companies such as ISACA groups that logically lead to the conclusion that conducting an IT audit is necessary for the management of information systems. The issue of training IT auditors, which must be certified and meet international standards, is acute.

Keywords: information system; information security, security concept, information security policy, threats, computer system, cyber audit; ICT; information protection; cyber threats

References

1 Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" of October 5, 2017 № 2163-VIII. Electronic resource. Access point: https://zakon.rada.gov.ua/laws/show/2163-19

2 Portal of the newspaper "Ukrainian Truth". Electronic resource. Access point: https://www.epravda.com.ua/publications/2016/12/9/613957/

3 Goskomzvyaz portal. Ways to solve the problem of information security in Ukraine. Electronic resource. Access point: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=CE0C98AFB4AE2CF71790756873D292F6?art_id=38826&cat_id=38712

4 Cherevko, O.V. (2020). Theoretical foundations of the concept of information security and classification of threats to the information security system. Effective economics, 5.

5 Kal'chenko, V.V. (2018). An overview of penetration testing methods for assessing the security of computer systems. Control, navigation and communication systems, 4, 109–114.

6 Semenenko, V.A. (2005). Information security. MGIU, Moscow, Russia: 215.

7 Kornjushin, P.N. (2003). Information security. TIDOT DVGU, Vladivostok, Russia: 154.

8 Konev, I.R. (2003). Information security. BHV-Peterburg, Saint Petersburg, Russia: 747.

9 Kavun, S.V. (2008). Information security. Vyd. KhNEU, Kharkiv, Ukraine: 352.

10 Anikin, I.V., Glova, V.I., Nejman, L.I. & Nigmatullina, A.N. (2008). The theory of information security and protection of information methodology. PH of Kazan gos. tehn. un-ta, Kazan, Russia: 358.

11 Sorokovskaja, A.A. (2010). Information security of the enterprise: new threats and prospects [Electronic resource]. – Access mode: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

12 Kurushin, V.D. & Mynaev, V.A. (2012). Computer crimes and information security. Novyj jurist, Moscow, Russia: 256.

13 Gatchin, Ju.A. (2010). The theory of information security and protection of information methodology. SPbGU ITMO, Saint Petersburg, Russia: 358.

14 Hajvorons'kyj, M.V. & Novikov, O.M. (2009). Safety of information and communication systems. Publishing house BHV, Russia: 608.

15 Dron', M.M., Malajchuk, V.P. & Petrenko, O.M. (2001). Bases of the theory of information protection. PH Dnipropetr. un-tu, Dnipropetrovsk, Ukraine: 312.

16 Danyk, Yu. H. & Suprunov, Yu. M. (2011). Some approaches to the formation of a training system for the cyber security system of Ukraine. Collection of scientific works of ZhVI NAU "Information systems", 5–22.

17 Minochkin, A.I. (2011). Information struggle: current state and experience of training specialists. Defense Bulletin, 2, 12–14.

18 Sysoyev, V. (2018). Analysis of the level of education and training of specialists in IT management and information security in Ukraine. [Electronic resource]. – Access mode: http://www.auditagency.com.ua/blog/ISACA_research_Education.pdf.

19 The first standard of higher education concerns cybersecurity. (2018). [Electronic resource]. Access mode: https://ligazakon.net/lawnews/doc/-nz173112-pershyy-standart-vyshchoyi-osvity-stosuyetsya-kiberbezpeky?type=ep.

20 Cybersecurity: A Generic Reference Curriculum (RC). (2016). Dear Partners/NATO Members, 4500-1 (OSEM PED)", 73.

21 "ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity", 50.

22 Center for Internet Security. (2019). CIS Controls Version 7. What's Old, What's New [Electronic resource]. Access mode: https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/.

23 Center for Internet Security. (2019). CIS Controls [Electronic resource]. Access mode: https://www.cisecurity.org/controls/.

Посилання на публікацію

APA *Kryvoruchko, Olena, Synichuk, Olena, Shvets, Denys, & Olexander, Minin. (2020). Analysis of the security status of information and telecommunication systems. Management of Development of Complex Systems, 42, 56 – 62, [in Ukrainian]; dx.doi.org\10.32347/2412-9933.2020.42.56-62.*

ДСТУ *Криворучко О.В. Аналіз стану захищеності інформаційно-телекомунікаційних систем [Текст] / О.В. Криворучко, О.М. Сунічук, Д.В. Швець, О.В. Мінін // Управління розвитком складних систем. – 2020. – № 42. – С. 56 – 62; dx.doi.org\10.32347/2412-9933.2020.42.56-62.*