МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 004.056.5

DOI: https://doi.org/10.32782/2520-2200/2018-5-35

Азєєв А.С.
аспірант кафедри маркетингу та бізнес-адміністрування
Одеського національного університету імені І.І. Мечникова

МЕТОДИКА ОЦІНКИ ТА ІДЕНТИФІКАЦІЇ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРИКЛАДІ ПОСЛУГИ ДИСТАНЦІЙНОГО НАВЧАННЯ

У статті розглядається методика та процес ідентифікації й оцінки (кількісно і якісно) ризику інформаційної безпеки. Проаналізовано наступні етапи в системі менеджменту інформаційної безпеки: визначення основних і допоміжних активів, загроз інформаційної безпеки та джерел їх походження, існуючих засобів і заходів контролю та управління ризиками; виявлення уразливостей інформаційної безпеки та визначення наслідків. У якості прикладу організації, до якої застосовується методика оцінки ризику, обрано компанію, що надає послуги дистанційного навчання. Сформовано зведену таблицю сценаріїв інцидентів інформаційної безпеки з їхніми наслідками, пов'язаними з активами й бізнесами-процесами.

Ключові слова: управління підприємством, бізнес-процес, інформаційна безпека, інформаційна система, загроза, оцінка ризику, ідентифікація ризику, вразливість, наслідки.

В статье рассматривается методика и процесс идентификации и оценки (количественной и качественной) риска информационной безопасности. Проанализировано следующие этапы в системе менеджмента информационной безопасности: определение основных и вспомогательных активов, угроз информационной безопасности и источников их возникновения, существующих стредств и мероприятий контроля и управления рисками; выявление уязвимостей информационной безопасности и определение последствий. В качестве организации, на примере которой применяется методика оценки риска, выбрана компания сферы услуг дистанционного обучения. Сформировано сводную таблицу сценариев инцидентов информационной безопасности с их последствиями, связанными с активами и бизнес-процессами.

Ключевые слова: управление предприятием, бизнес-процес, информационная безопасность, информационная система, угроза, оценка риска, идентифкация риска, уязвимость, последствия.

For the information age of the society, the process of implementing information technologies in all spheres of the economy is indispensable. Today the management of any organization operates with the corporate information on which the decision is made. Such information must comply with the requirements of relevance, probability, structuring, and, if necessary, confidentiality. Information technologies have become an attribute of increasing the efficiency of business processes, in particular, allowing business entities to reduce production costs, improve the accuracy of economic analysis, and correctly choose strategies and tactics in unforeseen circumstances. One of the most pressing problems that complicate the use of modern information technologies is the provision of information security. Building an effective system of information security depends primarily on the characteristics of risks, the probability of their occurrence and consequences. The article discusses the method and process of identifying and assessing (quantitative and qualitative) information security risk. The following stages in the information security management system were analyzed: identification of major and auxiliary assets, information security threats and their sources, existing funds, and risk control and management measures; identifying information security vulnerabilities and determining the consequences. As an organization, on the example of which the risk assessment methodology is applied, a company of distance learning services has been selected. Formed a summary table of information security incident scenarios with their consequences related to assets and business processes. The IS incident may affect more than one asset or only a part of an asset. The impact is related to the degree of success of the incident. As a result, there is an important difference between the value of the asset and the impact that results from the incident. The impact is considered as an immediate (operational) effect or a future (business) effect that includes financial and market consequences. The first assessment (without measures and means of control and management of any kind) will consider the impact as very close to the

value of the associated asset or a combination of assets. For each subsequent iteration for this asset, the impact will vary due to the availability and effectiveness of implemented measures and means of control and management. In the following, the methodology should be detailed according to the types of threats and relevant vulnerabilities. For more convenient use, it is necessary to turn to mathematical modelling and to create a user interface for a more convenient input of data.

Keywords: management of enterprise, business process, information security, information system, threat, risk assessment, identification of risk, vulnerability, consequences.

Постановка проблеми. Для інформаційної ери суспільства процес впровадження інформаційних технологій (ІТ) в усі сфери економіки є невід'ємним. Сьогодні керівництво будь-якого підприємства оперує корпоративною інформацією, на основі якої ухвалює рішення. Така інформація повинна відповідати вимогам актуальності, вірогідності, структурованості, і, якщо необхідно, конфіденційності.

ІТ стали атрибутом підвищення ефективності бізнес-процесів, зокрема, дозволяють господарюючим суб'єктам знизити витрати виробництва, підвищити точність економічного аналізу, правильно обирати стратегію й тактичні заходи в умовах непередбачених обставин. Однією з найбільш актуальних проблем, що ускладнюють застосування сучасних ІТ, є забезпечення інформаційної безпеки (ІБ) [1]. Побудова ефективної системи ІБ залежить насамперед від характеристики ризиків, ймовірності їх виникнення та наслідків.

Аналіз останніх досліджень і публікацій. Теоретичні аспекти формування інформаційного суспільства, інформаційних системи та ІБ висвітлені у працях Е. Тоффлера, С. П. Расторгуєва, Б. А. Кормича, В. А. Северина, В. К. Лєвіна, В. В. Райха, В. А. Тихонова та багатьох інших. Поточні статичні добірки та практичні дослідження можна почерпнути з матеріалів аналітичних відділень великих ІТ-корпорацій (IDC, Cisco, Symantec та ін.) та періодичні публікації, присвячені ІБ (Norton Cyber Security Report, ENISA Reports, Symantec Internet Security Threat Report тощо). В процесі активного вивчення знаходиться проблематика своєчасного виявлення курсу еволюції інформаційних загроз і ефективного реагування організації щодо мінімізації супутніх ризиків.

Мета статті: проаналізувати методику ідентифікації та оцінки ризиків ІБ на прикладі компанії, що надає послуги дистанційного навчання (ДН); дослідити співвідношення процесу ризик-менеджменту ІБ та компонентів процесу системи менеджменту ІБ.

Викладення основного матеріалу дослідження. Процедури оцінки ризику й обробки ризику в процесі менеджменту ризику ІБ можуть виконуватися ітеративно, такий підхід до проведення оцінки ризику може збільшити деталізацію і глибину оцінки при кожній наступній ітерації. Якщо для ефективного визначення дій вдається одержати достатню інформацію на черговому кроці ітерації, необхідну для зниження ризику до необхідного рівня, то вважається, що завдання етапу виконане. У випадку недостатності інформації для ухвалення рішення, переглядається контекст і здійснюється чергова ітерація оцінки ризику (критеріїв оцінки, впливу або прийняття ризиків), можливо для деякої окремої частини повної предметної області, яка обмежена першою точкою ухвалення рішення.

Ефективність обробки ризику безпосередньо залежить від результатів, що одержуються при оцінці ризику. Першочергова обробка ризику може не забезпечити необхідного рівня залишкового ризику. В цьому випадку можуть знадобитися, додаткові ітерації оцінки ризику зі зміною відповідних параметрів контексту, за кожною з яких відповідна до кроку ітерації процедура обробки ризику, що запускається на другій точці ухвалення рішення (рис. 1). Етапи управління ризиком регламентуються міжнародним стандартом ISO/IEC 31000 [2].

Спочатку виконаємо загальний опис оцінки ризику ІБ. Необхідно ідентифікувати ризики, кількісно або якісно їх охарактеризувати, призначити для них пріоритети відповідно до критеріїв оцінки ризику й цілями освітньої організації.

Ризик являє собою комбінацію наслідків, що випливають із небажаної події та ймовірності виникнення події [3; 14]. Оцінка ризику кількісно або якісно характеризує ризики й дає керівникам можливість призначати для ризиків пріоритети відповідно до усвідомленої керівництвом серйозності або інших встановлених критеріїв. Мета ідентифікації ризику – у визначенні того, що може відбутися при завданні можливих збитків, і в одержанні уявлення про те, як, де й чому міг мати місце такий збиток. Наступні нижче етапи, повинні поєднувати вхідні дані для діяльності кількісної оцінки ризику.

Визначимо активи, що входять у визначену сферу дії. Активом є щось, що має цінність для організації і тому потребує захисту. При визначенні активів необхідно враховувати, що інформаційна система складається не тільки з програмних і апаратних засобів. Щоб установити цінність активів, організація

повинна, у першу чергу, визначити всі належні їй активи на відповідному рівні деталізації.

Основними активами, як правило, є базові процеси й інформація про діяльність організації, що дистанційно виявляє освітні послуги в її сфері дії. Також можуть розглядатися й інші основні активи, такі як процеси життєдіяльності організації, які будуть мати відношення до формування політики ІБ або плану безперервності бізнесу. Залежно від мети, не завжди необхідний вичерпний аналіз усіх елементів, що складають процес ризик-менеджменту. У таких випадках сфера вивчення може бути обмежена найбільш значущими елементами. Допоміжним активам властиві вразливості, якими можуть скористатися загрози, націлені на псування основних активів області розгляду (процесів та інформації).

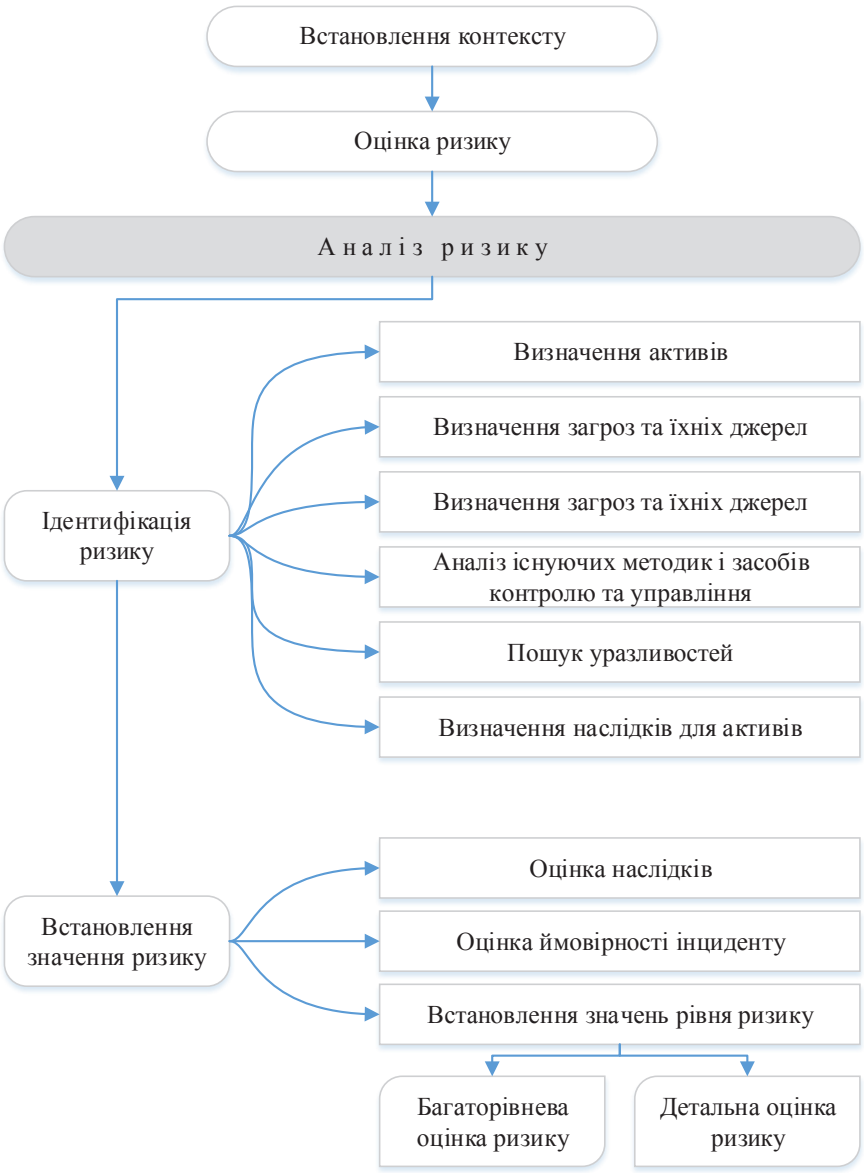

Рис. 1. Деталізований процес оцінки ризику ІБ

Визначення цінності активів полягає в узгодженні дійсної шкали цінностей і критеріїв для присвоєння кожному активу певного положення на шкалі, заснованого на визначенні цінності. Цінність деяких активів, може, встановлюватися суб'єктивно й ухвалювати рішення, можливо, будуть різні люди. Імовірні критерії, які використовуються для визначення цінності активу, включають його вихідну вартість, вартість його заміни чи відтворення, або цінність, що може бути абстрактною (цінність репутації організації).

Також основою для визначення цінності активів є видатки, які можуть бути понесені через втрату конфіденційності, цілісності, доступності в результаті інциденту.

Визначимо шкалу, яку будемо використовуватися. Як правило, використовується будь-яке число від 3 (наприклад, низький, середній і високий) до 10 відповідно до обраного організації підходом оцінки ризику.

Організація, які надає освітні послуги, в залежності від роду діяльності може встановити власні межі цінності активів, такі, як «високий», «середній», «низький». Ці межі оцінюються відповідно до обраних критеріїв (для можливих фінансових втрат межі повинні бути зазначені в грошовому вираженні, при розгляді загрози особистій безпеці, визначити грошову цінність може бути важко й неприйнятно).

Для системи ДН оберемо шкалу цінності активу від 0 до 4. Чим більш значимі й численні бізнес-процеси підтримуються активом, тим більша цінність цього активу. Повинна бути також визначена залежність одних активів від інших, оскільки це може впливати на їх цінність.

Інформація про залежності допоможе у визначенні загроз і особливо у виявленні враз-

Таблиця 1

Перелік активів та їхня цінність

Тип активу	Активи	Цінність активу
Основні активи		
Процес	Формування освітнього контенту. Комплекс послуг ДН. Звітність й оцінка роботи. Маркетинг та обслуговування Інтернет-ресурсів і системи ДН.	**3**
Інформація	Персональні дані учнів і персоналу. Фінансовий стан організації. Інформаційні ресурси бази даних освітніх електронних курсів.	**4**
Допоміжні активи		
Апаратні засоби	Сервери, персональні електронні пристрої з доступом до мережі Інтернет.	**4**
Програмні засоби	Операційна система. Антивірусні засоби. Програмне середовище для організації ДН. Браузери й плагіни для доступу до середовища ДН.	**2**
Мережа	Телекомунікаційні пристрої для з'єднання декількох фізично вилучених комп'ютерів або елементів інформаційної системи. Ретранслятори, мости, маршрутизатори, комутатори, концентратори. Мережне програмне забезпечення управління й моніторингу активного мережного устаткування. Генерація журналів реєстрації.	**3**
Персонал	Адміністрація організації, яка здійснює дистанційну освітню діяльність. Професорсько-викладацький колектив. Менеджери дистанційного освітнього процесу, фахівці навчальної частини, методисти, розробники освітнього контенту й контенту сайту освітньої організації. Персонал експлуатації інформаційної системи. Розробники програмних елементів середовища ДН і сайту освітньої організації.	**3**
Місце функціонування організації	Офісне та серверне приміщення. Зовнішній хостинг сайту. Точки віддаленого доступу до системи ДН.	**1**
Організація	Організаційна та функціональна структура організації.	**2**

ливостей. Крім того, це допоможе забезпечити правильне присвоєння значення цінності активам (завдяки взаємозв'язкам), демонструючи, таким чином відповідний рівень захисту.

Цінність активів, від яких залежать інші активи, може змінюватися в такий спосіб:

• якщо цінність залежних активів (наприклад, даних) нижче або дорівнює цінності розглянутого активу (наприклад, програмного забезпечення), його цінність не змінюється;

• якщо цінність залежних активів вище цінності розглянутого активу, його цінність має зрости відповідно до ступеня залежності або цінності інших активів.

Необхідно виявити випадкові, навмисні, природні джерела загроз. загрози можуть виходити як із самої організації, так і з джерел поза її межами.

Вхідні дані для визначення кількісної оцінки ймовірності виникнення загроз можуть бути отримані від власників активів або керівництва організації, користувачів, персоналу відділу кадрів, фахівців в області ІБ, фахівців юридичного відділу, експертів в галузі фізичної безпеки, та інших підрозділів, а також від метеорологічних служб, юридичних організацій, національних урядових закладів, страхових компаній. Під час аналізу загроз потрібно враховувати аспекти середовища й культури.

Списки загроз та їх статистику можна одержати від урядових структур, промислових підприємств, страхових компаній, юридичних організацій та ін.

У процесі оцінки загроз у системі ДН отриманий перелік загроз систематизований за видами загроз у таблиці 2. Для кожної загрози

Таблиця 2

Перелік загроз системи дистанційного навчання

Вид	Загрози	Походження
Фізичний збиток	Пожежа	В, Н, П
	Збиток, заподіяний водою	В, Н, П
	Руйнування встаткування або носіїв	В, Н, П
	Пил, корозія, замерзання	В, Н, П
Природні явища	Кліматичне явище	П
	Метеорологічне явище	П
Втрата важливих сервісів	Аварія системи кондиціювання повітря або водопостачання	В, Н
	Порушення енергопостачання	В, Н, П
	Відмова телекомунікаційного обладнання	В, Н
Перешкоди внаслідок випромінювання	Електромагнітне випромінювання	В, Н, П
	Теплове випромінювання	В, Н, П
	Електромагнітні імпульси	В, Н, П
Компрометація інформації	Перехоплення компрометуючих сигналів перешкод	Н
	Крадіжка носіїв або документів	Н
	Крадіжка обладнання	Н
	Розкриття	В, Н
	Дані з ненадійних джерел	В, Н
	Злочинне використання апаратних коштів	Н
	Злочинне використання програмного забезпечення	В, Н
	Визначення місцезнаходження	Н
Технічні несправності	Відмова обладанання	В
	Несправна робота встаткування	В
	Насичення інформаційної системи	В, Н
	Порушення функціонування програмного забезпечення	В
	Порушення супроводу інформаційної системи	В, Н
Несанкціоновані дії	Несанкціоноване використання обладнання	Н
	Шахрайське копіювання програмного забезпечення	Н
	Використання контрафактного або скопійованого програмного забезпечення	В, Н
	Викривлення даних	Н
	Незаконна обробка даних	Н
Компрометація функцій	Помилка при використанні	В
	Зловживання правами	В, Н
	Фальсифікація прав	Н
	Відмова в здійсненні дій	Н
	Порушення працездатності персоналу	В, Н, П

вказується її походження: «П» (природна), «Н» (навмисна), «В» (випадкова).

Щоб уникнути зайвої роботи або втрат, наприклад, при дублюванні засобів контролю, необхідно визначити існуючі заходи та засоби контролю та управління ІБ. Крім цього, при визначенні існуючих методик і засобів необхідно провести перевірку, щоб переконатися в правильності їхнього функціонування – процедура звертання до існуючих звітів по аудиту системи менеджменту ІБ повинна скорочувати час, який витрачається на вирішення цього завдання. Неналежне функціонування може стати причиною уразливості.

Одним зі способів кількісної оцінки дії засобів контролю є виявлення того, як знижується ймовірність виникнення загрози, ускладнюється використання уразливості й можливості впливу інциденту. Перевірки, проведені керівництвом, і звіти по аудиту також надають інформацію про ефективність існуючих методик і засобів контролю і керування.

Існуючий або плановий засоби можуть бути віднесені до розряду неефективних, недостатніх або необґрунтованих. Тоді їх слід піддати перевірці для визначення, чи підлягають вони заміні більш підходящими, видаленню, або можливо варто залишити їх через вартість.

Таблиця 3

Перелік сценаріїв інцидентів з їхніми наслідками, пов'язаними з активами й бізнесами-процесами

Перелік сценаріїв інцидентів	Загроза, що використовує вразливість	Вразливість	Активи й бізнес процеси	Операційні наслідки сценаріїв
1	2	3	4	5
З апаратними засобами	Порушення ремонтопридатності інформаційних систем	Недостатнє технічне обслуговування/неправильна установка носіїв даних	Сервери, персональні електронні устрої з доступом до мережі Інтернет.	– час на розслідування й відновлення; – упущені можливості; – репутація й інший «невловимий капітал».
	Погіршення стану носіїв даних	Відсутність програм періодичної заміни		
	Помилка у використанні	Відсутність ефективного контролю змін конфігурації		
	Втрата електроживлення	Чутливість до коливань напруги		
	Розкрадання носіїв даних або документів	Незахищене зберігання. Недбале (безвідповідальне) розміщення. Неконтрольоване копіювання.		
Із програмними засобами	Зловживання правами	Відсутнє або недостатнє тестування програмних засобів. Широко відомі дефекти програмних засобів. Відсутність «завершення сеансу» при роботі з АРМ. Списання або повторне використання носіїв даних без належного видалення інформації. Невірний розподіл прав доступу.	Операційна система. Антивірусні засоби. Програмне середовище для організації ДН. Браузери й плагіни до них для доступу до середовища ДН.	– час на розслідування й відновлення; – упущені можливості; – охорона праці й безпеки; – фінансові витрати на придбання специфічних навичок, необхідних для усунення несправності; – репутація й інший «невловимий капітал».
	Псування даних	Застосування прикладних програм для невідповідних даних.		
	Помилка у використанні	Складний користувацький інтерфейс. Відсутність документації. Неправильні параметри установки.		
	Фальсифікація прав	Відсутність механізмів ідентифікації й аутентифікації. Незахищені таблиці паролів. Поганий менеджмент паролів.		
	Нелегальна обробка даних	Активізація непотрібних сервісів.		
	Збій програмних засобів	Недопрацьоване або нове програмне забезпечення. Нечіткі або неповні специфікації для розробників. Відсутність ефективного контролю змін.		
	Приховані дії із програмними засобами	Неконтрольоване завантаження й використання програмних засобів. Відсутність резервних копій.		
	Розкрадання носіїв даних або документів	Відсутність фізичного захисту будівлі, дверей і вікон.		

Продовження таблиці 3

1	2	3	4	5
З мережею	Перехоплення інформації	Незахищені лінії зв'язку. Незахищений чутливий трафік.	Телекомунікаційні устрої, використані для з'єднання декількох фізично вилучених комп'ютерів або елементів інформаційної системи. Ретранслятори, мости, маршрутизатори, комутатори, концентратори. Мережне програмне забезпечення керування й моніторингу активного мережного встаткування. Генерація журналів реєстрації.	– час на розслідування й відновлення; – упущені можливості; – охорона праці й безпеки; – фінансові витрати на придбання специфічних навичок, необхідних для усунення несправності; – репутація й інший «невловимий капітал».
	Фальсифікація прав	Відсутність ідентифікації й аутентифікації відправника й одержувача.		
	Дистанційне шпигунство	Ненадійна мережна архітектура. Передача паролів у незашифрованому виді.		
	Перенасичення інформаційної системи	Неадекватний мережний менеджмент (стабільність маршрутизації).		
	Неавторизоване використання устаткування	Незахищені з'єднання мережі загального користування		
З персоналом	Порушення працездатності персоналу	Відсутність персоналу	Адміністрація організації. Професорсько-викладацький склад. Менеджери, фахівці навчальної частини, методисти, розробники освітнього контенту. Персонал з експлуатації й супроводу інформаційної системи. Розробники програмних елементів середовища ДН й сайту.	– упущені можливості; – охорона праці й безпеки; – фінансові витрати на придбання специфічних навичок, необхідних для усунення несправності;
	Руйнування устаткування або носіїв даних	Неадекватні процедури набору персоналу		
	Помилка у використанні	Недостатнє усвідомлення безпеки. Неналежне використання програмних і апаратних засобів. Відсутність поінформованості про безпеку.		
	Нелегальна обробка даних	Відсутність механізмів моніторингу.		
	Неавторизоване використання устаткування	Відсутність політик по правильному використанню телекомунікаційного середовища й обміну повідомленнями.		
З місцем функціонування організації	Погіршення стану носіїв даних	Неадекватне або недбале використання фізичного керування доступом до будинків і приміщенням.	Офіс і серверна. Зовнішній хостинг сайту. Точки віддаленого доступу до системи ДН.	– час на розслідування й відновлення; – охорони праці й безпеки.
	Розкрадання апаратури	Відсутність фізичного захисту будинку, дверей і вікон		
З організацією	Зловживання правами	Відсутність формального процесу для перегляду (нагляду) прав доступу. Відсутність або недостатні умови (дотичні безпеки) у договорах із клієнтами й/або третіми сторонами. Відсутність процедури, що стосується моніторингу засобів обробки інформації. Відсутність регулярних аудитів (нагляду). Відсутність процедур ідентифікації й оцінки ризику.	Організація, що виявляє освітні послуги. Структура організації: Адміністрація. Організаційно-методичний відділ. Відділ маркетингу. It-Відділ. Бухгалтерія.	– час на розслідування й відновлення; – упущені можливості; – охорони праці й безпеки; – фінансові витрати на придбання специфічних навичок, необхідних для усунення несправності; – репутація й інший «невловимий капітал».

Закінчення таблиці 3

1	2	3	4	5
З організацією	Порушення обслуговування інформаційної системи	Неадекватна відповідальність за технічне обслуговування. Відсутнє або незадовільна угода про рівень сервісу. Відсутність процедури контролю змін.	Організація, що виявляє освітні послуги. Структура організації: Адміністрація. Організаційно-методичний відділ. Відділ маркетингу. It-Відділ. Бухгалтерія.	– час на розслідування й відновлення; – упущені можливості; – охорони праці й безпеки; – фінансові витрати на придбання специфічних навичок, необхідних для усунення несправності; – репутація й інший «невловимий капітал».
	Псування даних	Відсутність формальної процедури контролю документації, що стосується системи менеджменту ІБ. Відсутність формальної процедури нагляду за записами системи менеджменту ІБ.		
	Дані з ненадійних джерел	Відсутність формального процесу санкціонування загальнодоступної інформації		
	Відмова в здійсненні діяльності	Відсутність належного розподілу обов'язків по забезпеченню ІБ		
	Відмова устаткування	Відсутність планів забезпечення безперервності бізнесу		
	Помилка у використанні	Відсутність політики використання електронної пошти. Відсутність процедур уведення програмного забезпечення в операційні системи. Відсутність обов'язків по забезпеченню ІБ в посадових інструкціях.		
	Нелегальна обробка даних	Відсутність або недостатні умови у договорах зі службовцями.		
	Розкрадання встаткування	Відсутність застереженого дисциплінарного процесу у випадку інциденту безпеки. Відсутність формальної політики по використанню портативних комп'ютерів. Відсутність контролю над активами, що перебувають за межами організації.		
	Розкрадання носіїв інформації або документів	Відсутня або незадовільна політика «чистого стола й порожнього екрана». Відсутність авторизації засобів обробки інформації. Відсутність установлених механізмів моніторингу порушень безпеки		
	Неавторизоване використання встаткування	Відсутність регулярних перевірок, проведених керівництвом. Відсутність процедур повідомлення про слабкі місця безпеки		
	Використання контрафактних або копійованих програмних засобів	Відсутність процедур, що забезпечують дотримання прав на інтелектуальну власність		

До заходів та засобів контролю й управління забезпечення ІБ системи ДН можна віднести:

• документування процесів менеджменту ІБ з метою доступності інформації про всі існуючі або плановані заходи і засоби, а також про стан їх реалізації;

• регулярний аналіз документів, що містять інформацію про заходи контролю й керування в тому числі планів обробки ризиків;

• перевірки, проведені разом зі співробітниками, відповідальними за ІБ (представником адміністрації, співробітником, відповідальним за безпеку програмної системи, охороною офісу, представниками професорсько-викладацького складу й представниками користувачів системи);

• регулярний обхід будівлі й огляд фізичних засобів контролю, порівняння існуючих засобів контролю з документованим списком, перевірка правильності та ефективності функціонування;

• аналіз результатів внутрішніх аудитів.

Необхідно виявити вразливості, які можуть бути використані загрозами для завдання збитків активам або організації. Наявність вразливості не завдає збитку саме по собі. Необхідна наявність загрози, яка зможе скористатися цією вразливістю. Для вразливості, якій не відповідає певна загроза, може не знадобитися впровадження засобу контролю й керування, але їй слід приділити увагу, моніторити на предмет змін. З іншого боку, загроза, якій не відповідає певна вразливість, може не приводити до ризику. Невірно реалізований, використаний, функціонуючий засіб управління і контролю може стати причиною вразливості. Ефективність або неефективність заходів і засобів керування й контролю може залежати від середовища, у якому вони функціонують.

Уразливості можуть бути пов'язані із властивостями активу, так як спосіб і мета використання активу в процесі надання освітньої послуги можуть відрізнятися від запланованих під час придбання або створення активу. Потрібно враховувати вразливості, що виникають із різних джерел, і які є зовнішніми й внутрішні стосовно активу.

Слід визначити наслідки для активів, викликані втратою конфіденційності, цілісності й доступності. Наслідком може бути зниження ефективності, несприятливі операційні умови, втрата бізнесу, збиток, нанесений репутації і т. д.

Ця діяльність визначає збиток або наслідки для організації, які можуть бути обумовлені сценарієм інциденту. Сценарій інциденту – це опис загрози, що використовує певну вразливість або сукупність вразливостей в інциденті ІБ [4]. Вплив сценаріїв інцидентів обумовлюється критеріями впливу, обумовленими в ході діяльності встановлення контексту. Вплив може торкатися одного або кількох активів, а також частини активу. Тому активам може призначатися цінність, обумовлена як їх фінансовою вартістю, так і наслідками для бізнесу у випадку їх псування або компрометації. Наслідки можуть бути тимчасовими або постійними, як це буває у випадку руйнування активів.

Висновки. Отже, інцидент ІБ може впливати більш ніж на один актив або тільки на частину активу. Вплив пов'язаний із ступенем успішності інциденту. Як наслідок, існує важлива відмінність між цінністю активу й впливом, що є результатом інциденту. Вплив розглядається як негайний (операційний) ефект, або майбутній (бізнес-) ефект, який включає фінансові й ринкові наслідки. Перша оцінка (без заходів і засобів контролю й керування будь-якого роду) буде розглядати вплив як дуже близький до цінності пов'язаного із цим активу або комбінації активів. При кожній наступній ітерації для цього активу вплив буде відрізнятися внаслідок наявності й ефективності реалізованих заходів і засобів контролю й керування.

Надалі методику слід деталізувати за типами загроз та відповідних уразливостей. Для більш зручного використання варто звернутися до математичного моделювання та створити користувацький інтерфейс для більш зручного вводу даних.

Список використаних джерел:

1. Азєєв А. С. Сучасні напрямки типологізації інформаційних загроз та тренди ринку інформаційної безпеки [Електронний ресурс] / А. С. Азеев, М. П. Чайковська // Електронне фахове видання. Мукачівський державний університет. Економіка та суспільство. 2017. № 13. URL: www.economyandsociety.in.ua/index.php/journal-13
2. ISO 31000 – Risk management. URL: www.iso.org/iso-31000-risk-management.html
3. OHSAS 18001:2007 // Перевод на русский язык и научно-техническое редактирование В. А. Качалов. – СЕРТ Менеджмент, 2007. 34 с.
4. ISO/IEC 27035, Information technology – Information security incident management. URL: www.iso.org/standard/60803.html.