АНОТАЦІЯ

Метою цієї роботи є дослідження методів підвищення ефективності управління ризиками інформаційної безпеки підприємства та вибір і обґрунтування найоптимальніших методів для некомерційних комунальних підприємств у сфері охорони здоров’я.

Об’єктом дослідження є регулювання відносин у сфері захисту інформації з обмеженим доступом на підприємствах, в установах, організаціях.

Предметом роботи є методи підвищення ефективності управління ризиками інформаційної безпеки підприємства. Роботу виконано для пробації в некомерційних комунальних підприємств у сфері охорони здоров’я.

Основними методами, які використано в роботі є аналіз, синтез, структурний метод і метод порівняння. Здійснено поділ спеціальних методів на якісні, кількісні та змішані.

За результатами дослідження приходимо до висновків про методичну обґрунтованість і економічну доцільність реалізації системи управління ризиками кібербезпеки для некомерційного комунального підприємства у сфері охорони здоров’я на основі стандартів ISO/IEC TR 13335.

Приходимо до висновків, що що система управління ризиками на основі стандарту ISO/IEC TR 13335 є виправданою для некомерційних комунальних підприємств

Результати магістерської роботи підлягають практичному застосуванню для запровадження ефективної системи управління ризиками інформаційної безпеки під час реорганізації з закладів охорони здоров’я на комунальні некомерційні підприємства, яка відбувається у рамках медичної реформи і децентралізації. В подальшому результати цього дослідження можуть використовуватися для вдосконалення управління ризиками кібербезпеки існуючих комунальних некомерційних підприємств у сфері охорони здоров’я.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНИХ СИСТЕМ

ABSTRACT

The purpose of this work is to investigate methods for improving the efficiency of enterprise information security risk management and to select and justify the best methods for non-profit public utility companies in the healthcare sector.

The object of the study is the regulation of relations in the field of protection of information with restricted access in enterprises, institutions, organizations.

The subject of work is methods of increasing the efficiency of information security risk management of the enterprise. The work was done for probation in a non-profit public utility company in the healthcare sector.

The main methods used in the work are analysis, synthesis, structural method and comparison method. Special methods are divided into qualitative, quantitative and mixed methods.

According to the results of the study, we come to the conclusions about the methodological validity and economic feasibility of implementing a cybersecurity risk management system for a non-profit health care utility based on ISO / IEC TR 13335 standards.

We conclude that the ISO / IEC TR 13335 risk management system is justified for non-profit utility companies

The results of the master's thesis are subject to practical application for the implementation of an effective system of information security risk management during the reorganization from healthcare facilities to municipal non-profit enterprises undergoing medical reform and decentralization. In the future, the results of this study can be used to improve the cybersecurity risk management of existing community-based nonprofit healthcare businesses.

Keywords: ENTERPRISE INFORMATION SECURITY, INFORMATION SECURITY RISKS, INFORMATION SECURITY MANAGEMENT, RISK CHEMISTRY MANAGEMENT METHODS

Вступ 7

1 Структура інформаційної безпеки 9

1.1 Загальні відомості про інформаційну безпеку 9

1.2 Загрози в інформаційній безпеці 13

1.3 Загальні відомості про ризики та управління ними 28

2. Структура інформаційної системи підприємства, ризики та загрози 36

2.1 Інформаційні системи та кібербезпека крізь призму системного підходу до управління бізнесом 36

2.2 Структурний аналіз інформаційного середовища та загальна характеристика ризиків кібербезпеки підприємства 41

2.3 Управління ризиками у процесі обробки інформації 51

Висновки до розділу 53

3. Методи аналізу ризиків інформаційної системи підприємства 55

3.1 Загальна характеристика методології аналізу ризиків інформаційної безпеки 55

3.2. Методи та стандарти аналізу інформаційної системи 56

3.3 Реалізація системи управління ризиками безпекинекомерційного комунального підприємства на основі стандарту ISO/IEC TR 13335 65

3.4 Висновки до розділу 68

4 Розробка моделі порушника 69

4.1 Теоритичні відомості 69

4.2 Реалізація моделі порушника 69

4.3 Висновки до розділу 72

5 Обґрунтування економічної ефективності 73

5.1 Мета та завдання 73

5.2 Розрахунок витрат на впровадження системи управління ризиками інформаційної безпеки підприємства 74

5.2 Розрахунок норм часу на виконання науково-дослідної роботи 75

5.3 Висновки до розділу 77

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 78

6.1 Вимоги щодо приміщення та робочих місць 78

6.2.1 Основні положення про надзвичайні ситуації 83

6.2.2 Планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації 85

Висновки до розділу 87

7 ЕКОЛОГІЯ 88

7.1 Енергозбереження і його роль у вирішенні екологічних проблем. 88

7.2 Статистика екологічних показників 91

Висновки 94

Бібліографія 96

ВСТУП

Актуальність теми дослідження. На початку 2018 року в Україні в рамках медичної реформи розпочато реорганізацію (перетворення) закладів охорони здоров'я у неприбуткові комунальні підприємства. Створення та подальше функціонування відповідних підприємств передбачає використання значного обсягу різноманітної інформації, від персональних даних пацієнтів та медичного персоналу і до відомостей у сфері бухгалтерського обліку. Значна частина інформації, яка звичайно використовується (буде використовуватися) у діяльності неприбуткових комунальних підприємств у галузі охорони здоров'я, містить охоронювану законодавством лікарську (медичну) таємницю. З огляду на це, ефективне управління ризиками інформаційної безпеки відповідних підприємств є безпрецедентно важливим, а дослідження цієї теми – актуальним.

Метою цієї роботи є дослідження методів підвищення ефективності управління ризиками інформаційної безпеки підприємства та вибір і обґрунтування найоптимальніших методів для некомерційних комунальних підприємств у сфері охорони здоров'я.

Досягненню мети дослідження слугували наступні **завдання**:

— розглянути структуру інформаційної безпеки підприємства;
— дослідити поняття та види загроз у інформаційній безпеці;
— проаналізувати загальні положення про ризики інформаційних систем та управління ними;
— розглянути інформаційні системи та кібербезпеку крізь призму системного підходу до управління бізнесом;
— здійснити структурний аналіз інформаційного середовища та ризиків інформаційної безпеки підприємства;
— охарактеризувати методи аналізу ризиків інформаційної безпеки;
— розглянути методи та стандарти аналізу інформаційної системи;
— обґрунтувати реалізацію системи управління ризиками кібербезпеки для некомерційного комунального підприємства у сфері охорони здоров'я на основі стандартів ISO/IEC TR 13335.

Об'єктом дослідження є регулювання відносин у сфері захисту інформації з обмеженим доступом на підприємствах, в установах, організаціях.

Предметом дослідження є методи підвищення ефективності управління ризиками інформаційної безпеки підприємства. Роботу виконано на прикладі некомерційних комунальних підприємств у сфері охорони здоров'я.

Методами які використано в роботі є аналіз, синтез, структурний метод і метод порівняння. Здійснено поділ спеціальних методів на якісні, кількісні та змішані.

Наукова новизна цього дослідження полягає у впровадженні методів підвищення ефективності управління ризиками інформаційної безпеки бізнесу для новостворених некомерційних комунальних підприємств у галузі охорони здоров'я.

Результати цієї роботи можуть бути практично використані для запровадження ефективної системи управління ризиками інформаційної безпеки під час реорганізації закладів охорони здоров'я з комунальних установ на комунальні некомерційні підприємства, яка відбувається у рамках реформи фінансування медицини. В подальшому результати цього дослідження можуть використовуватися для вдосконалення управління ризиками кібербезпеки існуючих комунальних некомерційних підприємств у сфері охорони здоров'я і медичних установ в цілому, не обов'язково комунальної форми власності.

Особистий внесок здобувача полягає в перенесенні існуючих методів підвищення ефективності управління ризиками та новостворені некомерційні комунальні підприємства з урахуванням міжнародних стандартів безпеки.

Апробація результатів магістерської роботи. Основні результати роботи доповідалися на VII науково-технічній конференції «Інформаційні моделі, системи та технології».

1 СТРУКТУРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Загальні відомості про інформаційну безпеку

Інформаційна безпека – це захищеність інформації (даних), програмного забезпечення і устаткування від випадкових та навмисних шкідливих впливів природного, технічного, антропогенного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації і підтримуючої інфраструктури.

Захист інформації - це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Правильний з методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем. Загрози інформаційній безпеці - це зворотна сторона використання інформаційних технологій. Трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно відрізнятися[36].

Інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це принципово ширше поняття. Суб'єкт інформаційних відносин може постраждати (зазнати збитків та/або отримати моральну шкоду) не тільки від несанкціонованого доступу, але і від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій (наприклад, навчальних закладів) власне захист від несанкціонованого доступу до інформації стоїть за важливістю зовсім не на першому місці.

Повертаючись до питання термінології, відзначимо, що термін "комп'ютерна безпека", часто вживаний як контекстуальний синонім інформаційної безпеки, на нашу думку, є занадто вузьким. Комп'ютери - тільки одна зі складових інформаційних систем, і хоча наша увага буде зосереджена в першу чергу на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в

першу чергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється користувач.

Згідно з визначенням інформаційної безпеки, вона залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електричного та теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою її функцій [13].

Очевидно, застрахуватися від усіх видів збитку неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує розміру потенційного збитку. Значить, з чимось доводиться миритися і захищатися слід тільки від того, з чим змиритися ніяк не можна. Іноді таким неприпустимим збитком є нанесення шкоди здоров'ю людей або стану навколишнього середовища, але частіше поріг неприйнятності має матеріальний (грошовий) вираз, а метою захисту інформації стає зменшення розмірів збитку до допустимих значень.

Інформаційна безпека - багатогранна, можна навіть сказати, багатовимірна область діяльності, в якій успіх може принести тільки системний, комплексний підхід.Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна розділити на наступні категорії: забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів та підтримуючої інфраструктури. Іноді до основних складових інформаційної безпеки включають також захист від несанкціонованого копіювання інформації [36].

Пояснимо поняття доступності, цілісності і конфіденційності. Доступність – це властивість інформації яка полягає в тому що користувач або процес, який володіє повноваженнями може використовувати інформацію відповідно до політики безпеки та прав доступу до інформації. Під цілісністю мається на увазі властивість інформації, що забезпечує її захищеність від руйнування і несанкціонованої модифікації. Конфіденційність – це властивість

інформації яка полягає в унеможливленні несанкціонованого доступу до інформації.

Інформаційні системи створюються (запроваджуються) для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає шкоди всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.Особливо яскраво провідна роль доступності виявляється в різного роду системах управління - виробництвом, транспортом тощо.

Цілісність можна поділити на статичну (що розуміється як незмінність інформаційних об'єктів) і динамічну (що відноситься до коректного виконання складних дій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки або дублювання окремих повідомлень.

Цілісність виявляється найважливішим аспектом інформаційної безпеки в тих випадках, коли інформація служить інструкцією для дій. Рецептура ліків, наказані медичні процедури, набір і характеристики комплектуючих виробів, хід технологічного процесу - все це приклади інформації, порушення цілісності якої може стати в буквальному сенсі смертельним. Значної шкоди може завдати і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера якої-небудь урядової організації [26].

В Україні найбільший науковий і практичний інтерес характерний для критерію (ознаки) конфіденційності інформаційних систем. Проте фактичний стан справ із забезпеченням конфіденційності все ж залишає бажати кращого. По-перше, відомості про технічні канали просочування інформації є закритими, так що більшість користувачів позбавлена можливості скласти уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони і технічні проблеми.

Інформаційна безпека є одним з найважливіших аспектів інтегральної безпеки, на якому б рівні ми не розглядали останню - національному, галузевому, корпоративному або персональному. Наведемо декілька прикладів.

Так, за розпорядженням президента США Клінтона у липні 1996 року була створена Комісія з захисту критично важливої інфраструктури. Ішлося про захист як від фізичних нападів, так і від кібер-атак. Трохи більше року потому, доповідаючи перед президентом, голова комісії Робер Марш заявив, що на даний час ні уряд, ні приватний сектор здебільшого не вживають комплексу заходів для попередження кібер-атак [4].

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку даного аспекту безпеки, яка полягає в тому, що інформаційна безпека є складова частина інформаційних технологій - області, що розвивається безпрецедентно високими темпами. Відтак, у сфері забезпечення безпеки інформаційних систем важливі не стільки окремі рішення, скільки механізми генерації нових рішень, що дозволяють жити в темпі технічного прогресу.

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення інформаційної безпеки. Слід виходити з того, що необхідно конструювати надійні системи (інформаційної безпеки) із залученням ненадійних компонентів (програм). В принципі, це можливо, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом усього життєвого циклу інформаційної системи [39].

У таких умовах системи інформаційної безпеки повинні вміти протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим. Іноді напад триває долі секунди; деколи з’ясування вразливих місць ведеться поволі і розтягується, так що підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових інформаційної безпеки - доступності, цілісності або конфіденційності.

1.2 Загрози в інформаційній безпеці

Знання можливих загроз, а також уразливих місць захисту, які ці загрози зазвичай експлуатують, необхідно для того, щоб вибирати найбільш економічні засоби забезпечення безпеки.Загроза - це потенційна можливість певним чином порушити інформаційну безпеку.Спроба реалізації загрози називається атакою, а той, хто вживає таку спробу, - зловмисником. Потенційні зловмисники називаються джерелами загрози.

Найчастіше загроза є наслідком наявності вразливих місць в захисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до устаткування або помилки у програмному забезпеченні).

Проміжок часу від моменту, коли з'являється можливість використовувати вразливе місце, і до моменту, коли відповідна вразливість ліквідовується, називається вікном небезпеки. Поки існує вікно небезпеки, можливі успішні атаки на інформаційну систему.

Ми вже вказували, що нові вразливі місця з'являються постійно. Це наводить на два висновки:

— по-перше, вікна небезпеки існують практично завжди;
— по-друге, відстеження вікон небезпеки має проводитися безперервно і систематично.

Відзначимо, що деякі загрози не можна вважати наслідком якихось помилок чи прорахунків; вони існують в силу самої природи сучасних інформаційних систем. Наприклад, загроза відключення електрики або виходу параметрів струму за допустимі межі існує в силу залежності апаратного забезпечення інформаційних систем від якісного електроживлення [36].

Розглянемо найбільш поширені загрози, до яких схильні сучасні інформаційні системи. Мати уявлення про можливі загрози, а також про вразливі місця, які ці загрози зазвичай експлуатують, необхідно для того, щоб вибирати найбільш ефективні засоби забезпечення безпеки. Занадто багато міфів існує в сфері інформаційних технологій, тому незнання в даному випадку веде до

перевитрати коштів і, що ще гірше, до концентрації ресурсів там, де вони не особливо потрібні, за рахунок ослаблення дійсно вразливих напрямків.

Підкреслимо, що саме поняття "загроза" в різних ситуаціях часто трактується по-різному. Наприклад, для підкреслено відкритої організації загроз конфіденційності може просто не існувати - вся інформація вважається загальнодоступною; проте в більшості випадків нелегальний доступ представляється серйозною небезпекою. Іншими словами, загрози, як і все інше у інформаційній безпеці, залежать від інтересів суб'єктів інформаційних відносин (і від того, який збиток є для них неприйнятним). Втім, багато загроз (наприклад, пожежі) небезпечні для всіх [47].

Загрози можна класифікувати за кількома критеріями:

— по аспекту інформаційної безпеки (доступність, цілісність, конфіденційність), проти якого загрози спрямовані в першу чергу;
— по компонентах інформаційних систем, на які загрози націлені (дані, програми, апаратура, підтримуюча інфраструктура);
— за способом здійснення (випадкові/навмисні, дії природного/техногенного характеру);
— по розташуванню джерела загроз (всередині/поза інформаційною системою) [36].

В якості основного критерію ми будемо використовувати перший, по аспекту інформаційної безпеки, залучаючи, при необхідності, інші. Найчастішими є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи.Інколи такі помилки і є власне загрозами (неправильно введені дані або помилка в програмі, що викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (помилки адміністрування). За деякими даними, до 65% втрат - наслідок ненавмисних помилок.

Пожежі та повені не приносять стільки бід, скільки безграмотність і недбалість у роботі. Очевидно, самий радикальний спосіб боротьби з ненавмисними помилками - максимальна автоматизація і строгий контроль.

Інші загрози доступності класифікуємо за компонентами ІС, на які націлені загрози:

— відмова користувачів;
— внутрішня відмова інформаційної системи;
— відмова підтримуючої інфраструктури.

Зазвичай щодо користувачів розглядаються наступні загрози:

— небажання працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості і при розходженні між запитами користувачів і фактичними можливостями та технічними характеристиками);
— неможливість працювати з системою через відсутність відповідної підготовки (нестача загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією тощо);
— неможливість працювати з системою в силу відсутності технічної підтримки (неповнота документації, недолік довідкової інформації та інше).

Основними джерелами внутрішніх відмов є:

— відступ (випадковий або навмисний) від встановлених правил експлуатації;
— вихід системи з штатного режиму експлуатації в силу випадкових або навмисних дій користувачів або обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації тощо);
— помилки при конфігуруванні системи;
— відмови програмного і апаратного забезпечення;
— руйнування даних;
— руйнування або пошкодження апаратури [68].

По відношенню до підтримуючої інфраструктури рекомендується розглядати наступні загрози:

— порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо-та / або теплопостачання, кондиціонування;
— руйнування або пошкодження приміщень;
— неможливість або небажання обслуговуючого персоналу та / або користувачів виконувати свої обов'язки.

Досить небезпечні так звані «скривджені» співробітники - нинішні і колишні. Часто вони прагнуть завдати шкоди організації – «кривднику», наприклад:

— зіпсувати обладнання;
— вбудувати логічну бомбу, яка з часом зруйнує програми та/або дані;
— видалити дані.

Колишні співробітники знайомі з порядками в організації і здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу (логічного та фізичного) до інформаційних ресурсів анулювалися [25].

Небезпечні, зрозуміло, стихійні лиха та події, що сприймаються як стихійні лиха, - пожежі, повені, землетруси, урагани. За статистикою, на частку вогню, води і тому подібних «зловмисників» (серед яких найпоширеніший - перебій електроживлення) припадає 13% втрат, завданих інформаційним системам.

Загрози доступності можуть виглядати грубо - як ушкодження або навіть руйнування обладнання (в тому числі носіїв даних). Таке пошкодження може викликатися природними причинами (найчастіше - грозами). На жаль, масово розповсюджені на сьогодні джерела безперебійного живлення не захищають від потужних короткочасних імпульсів, і випадки вигоряння устаткування - не рідкість.

В принципі, потужний короткочасний імпульс, здатний зруйнувати дані на магнітних носіях, можна згенерувати і штучним чином - за допомогою так званих високоенергетичних радіочастотних гармат. Але, напевно, в наших умовах подібну загрозу варто все ж визнати надуманою.

Дійсно небезпечні протікання водопроводу і опалювальної системи. Часто організації, щоб заощадити на орендній платі, знімають приміщення в будинках старої споруди, роблять косметичний ремонт, але не змінюють старі комунікації. Влітку, в сильну спеку, схильні ламатися кондиціонери, встановлені

в серверних залах, набитих дорогим обладнанням. У результаті значної шкоди наноситься і репутації, і коштам організації [36].

Загальновідомо, що періодично необхідно проводити резервне копіювання даних. Однак навіть якщо ця пропозиція виконується, резервні носії часто зберігають недбало (до цього ми ще повернемося при обговоренні загроз конфіденційності), не забезпечуючи їх захист від шкідливого впливу навколишнього середовища.

Перейдемо тепер до загроз доступності, перш за все – до програмних атак на доступність. В якості засобу виведення системи з штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай - смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). За розташуванням джерела загрози таке споживання поділяється на локальне і віддалене. При прорахунках в конфігурації системи локальна програма здатна практично монополізувати процесор або фізичну пам'ять, звівши швидкість виконання інших програм до нуля.

Найпростіший приклад віддаленого споживання ресурсів - атака, що отримала найменування «SYN-повінь». Вона являє собою спробу переповнити таблицю «напіввідкритих» TCP-з'єднань сервера (встановлення з'єднань починається, але не закінчується). Така атака щонайменше ускладнює встановлення нових з’єднань з боку легальних користувачів, тобто сервер виглядає як недоступний [7].

По відношенню до атаки «Papa Smurf» уразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на такі пакети «з'їдають» смугу пропускання.

Віддалене споживання ресурсів останнім часом проявляється в особливо небезпечній формі - як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю спрямовуються цілком легальні запити на з'єднання та/або обслуговування. Часом початку «моди» на подібні атаки можна вважати лютий 2000 року, коли жертвами виявилися кілька найбільших систем електронної комерції (точніше - власники і користувачі систем).

Відзначимо, що якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною спроможністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність вкрай важко [4].

Для виведення систем зі штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних та апаратних помилок. Наприклад, відома помилка в процесорі Pentium I дає можливість локальному користувачеві шляхом виконання певної команди «підвісити» комп'ютер, так що допомагає тільки апаратний RESET. Програма «Teardrop» віддалено «підвішує» комп'ютери, експлуатуючи помилку в збірці фрагментованих IP-пакетів [9].

Одним із найнебезпечніших способів проведення атак є впровадження в системи, що атакуються, шкідливого програмного забезпечення.

Ми виділимо наступні межі шкідливого програмного забезпечення:

— шкідлива функція;
— спосіб розповсюдження;
— зовнішнє уявлення.

Частина, що здійснює руйнівну функцію, будемо називати «бомбою». Взагалі кажучи, спектр шкідливих функцій необмежений, оскільки «бомба», як і будь-яка інша програма, може володіти як-завгодно складною логікою, але зазвичай «бомби» призначаються для:

— впровадження іншого шкідливого програмного забезпечення;
— отримання контролю над системою, яка атакується;
— агресивного споживання ресурсів;
— зміни або руйнування програм або даних.

По механізму розповсюдження розрізняють:

— віруси-коди, що володіють здатністю до поширення (можливо, зі змінами) шляхом впровадження в інші програми;
— "черв'яки" - код, здатний самостійно, тобто без впровадження в інші програми, викликати поширення своїх копій по інформаційній системі та їх виконання (для активізації вірусу потрібно запуск зараженої програми).

Віруси-коди зазвичай поширюються локально, в межах вузла мережі; для передачі по мережі їм потрібна зовнішня допомога, така як пересилання зараженого файлу. «Черв'яки», навпаки, орієнтовані в першу чергу на пересування по мережі.

Іноді саме поширення шкідливого програмного забезпечення викликає агресивне споживання ресурсів і, отже, є шкідливою функцією. Наприклад, «черв'яки» «з'їдають» смугу пропускання мережі і ресурси поштових систем. З цієї причини для атак на доступність вони не потребують вбудовування спеціальних «бомб».

Шкідливий код, який виглядає як функціонально корисна програма, називається троянським конем, або трояном. Наприклад, звичайна програма, будучи ураженою вірусом, стає троянською; деколи троянські програми виготовляють вручну і підсовують довірливим користувачам у привабливій упаковці.

Вікно небезпеки щодо шкідливого програмного забезпечення з'являється з випуском нового різновиду «бомб», вірусів-кодів або «черв'яків» і перестає існувати з оновленням бази даних антивірусних програм [36].

За традицією, з усього шкідливого програмного забезпечення найбільшу увагу громадськості приділено вірусам. Дотримання нескладних правил «комп'ютерної гігієни» практично зводить ризик зараження до нуля. Там, де працюють згідно равил, число заражених комп'ютерів складає зазвичай лише долі відсотка.

У 1999 році, з появою вірусу "Melissa", ситуація кардинальним чином змінилася. "Melissa" - це макровірус для файлів MS-Word, що поширюється за допомогою електронної пошти в приєднаних файлах. Коли такий (заражений) приєднаний файл відкривають, він розсилає свої копії по перших 50 адресах з адресної книги Microsoft Outlook. В результаті поштові сервери піддаються атаці на доступність [9].

Як вже говорилося, пасивні об'єкти відходять у минуле; так званий активний вміст стає нормою. Файли, які за всіма ознаками мали б ставитися до

даних (наприклад, документи у форматах MS-Word або Postscript, тексти поштових повідомлень), здатні утримувати інтерпретуються компоненти, які можуть запускатися неявним чином при відкритті файлу. Як і всяке в цілому прогресивне явище, таке "підвищення активності даних" має свій зворотний бік (у розглянутому випадку - відставання у розробці механізмів безпеки і помилки в їх реалізації). Звичайні користувачі ще не скоро навчаться застосовувати інтерпретуються компоненти "у мирних цілях" (або хоча б дізнаються про їх існування), а перед зловмисниками відкрилося по суті необмежене поле діяльності [25].

Інтеграція різних сервісів, наявність серед них мережевих, загальна зв'язність багаторазово збільшують потенціал для атак на доступність, полегшують поширення шкідливого програмного забезпечення (вірус «Melissa» - класичний тому приклад).

Як це часто буває, услід за «Melissa» з'явилася на світ ціла серія вірусів, «черв'яків» і їх комбінацій: «Explorer.zip» (червень 1999), «BubbleBoy» (листопад 1999), «ILOVEYOU» (травень 2000) та інші. Не те що б від них був особливо великий збиток, але суспільний резонанс вони викликали чималий [9].

Активний вміст, крім інтерпретуються компонентів документів та інших файлів даних, має ще однин популярний інтерфейс - так звані мобільні агенти. Це програми, які завантажуються на інші комп'ютери і там виконуються. Найбільш відомі приклади мобільних агентів - Java-аплети, що завантажуються на комп'ютер користувача і інтерпретовані Internet-навігаторами. Виявилося, що розробити для них модель безпеки, що залишає достатньо можливостей для корисних дій, не так-то просто; ще складніше реалізувати таку модель без помилок. У серпні 1999 року стали відомі недоліки в реалізації технологій ActiveX і Java в рамках Microsoft Internet Explorer, які давали можливість розміщувати на Web-серверах шкідливі аплети, що дозволяють одержувати повний контроль над системою-візитером.

Для впровадження «бомб» часто використовуються помилки типу «переповнення буферу», коли програма, працюючи з областю пам'яті, виходить

за межі допустимого і записує в потрібні зловмисникові місця певні дані. Так діяв ще в 1988 році знаменитий «черв'як Моріса»; у червні 1999 року хакери знайшли спосіб використовувати аналогічний метод по відношенню до Microsoft Internet Information Server (IIS), щоб отримати контроль над Web-сервером. Вікно небезпеки охопило відразу близько півтора мільйонів серверних систем.

Не забуті сучасними зловмисниками і випробувані троянські програми. Наприклад, трояни Back Orifice і Netbus дозволяють отримати контроль над користувацькими системами з різними варіантами MS-Windows [4].

Таким чином, дія шкідливого програмного забезпечення може бути спрямована не тільки проти доступності, але і проти інших основних аспектів інформаційної безпеки.

На другому місці за розмірами збитку (після ненавмисних помилок і упущень) стоять крадіжки і підробки. За даними газети USA Today, ще в 1992 році в результаті подібних протиправних дій з використанням персональних комп'ютерів американським організаціям було завдано загальний збиток у розмірі 882 мільйонів доларів. Можна припустити, що реальний збиток був набагато більше, оскільки багато організацій зі зрозумілих причин приховують такі інциденти; не викликає сумнівів, що в наші дні збиток від такого роду дій виріс багаторазово [7].

У більшості випадків винуватцями виявлялися штатні співробітники організацій, відмінно знайомі з режимом роботи і заходами захисту. Це ще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про них значно менше, ніж про зовнішні.

Раніше ми проводили різницю між статичною та динамічною цілісністю. З метою порушення статичної цілісності зловмисник (як правило, штатний співробітник) може:

— ввести неправильні дані;
— змінити дані.

Потенційно уразливі з точки зору порушення цілісності не тільки дані, але й програми.

Загрозами динамічної цілісності є порушення транзакцій, крадіжка, дублювання даних або внесення додаткових повідомлень (мережевих пакетів тощо). Відповідні дії в мережевому середовищі називаються активним прослуховуванням.

Конфіденційну інформацію можна розділити на предметну і службову. Службова інформація (наприклад, паролі користувачів) не відноситься до визначеної предметної області, в інформаційній системі вона грає технічну роль, але її розкриття особливо небезпечне, оскільки воно загрожує отриманням несанкціонованого доступу до всієї інформації, в тому числі предметної.

Навіть якщо інформація зберігається в комп'ютері або призначена для комп'ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер.

Багатьом людям доводиться виступати в якості користувачів не однієї, а цілого ряду систем (інформаційних сервісів). Якщо для доступу до таких систем використовуються багаторазові паролі чи інша конфіденційна інформація, то напевно ці дані будуть зберігатися не тільки в голові, але і в записнику або на листках паперу, які користувач часто залишає на робочому столі, а то й просто втрачає. І справа тут не в неорганізованості людей, а в недоліках парольної схеми. Неможливо пам'ятати багато різних паролів; рекомендації по їх регулярній зміні тільки погіршують становище, змушуючи застосовувати нескладні схеми чергування або взагалі намагатися звести справу до двох-трьох легких паролів [36].

Описаний клас вразливих місць можна назвати розміщенням конфіденційних даних у середовищі, де їм не забезпечено (найчастіше - і не може бути забезпечено) необхідний захист. Крім паролів, що зберігаються в записниках користувачів, в цей клас потрапляє передача конфіденційних даних у відкритому вигляді (в розмові, в листі, по мережі), яка робить можливим перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування

мережі тощо), але ідея одна - здійснити доступ до даних в той момент, коли вони найменш захищені.

Загрозу перехоплення даних слід брати до уваги не тільки при початковому конфігуруванні інформаційних систем, але і, що дуже важливо, при всіх змінах. Вельми небезпечною загрозою є виставки, на які багато організацій, недовго думаючи, відправляють обладнання з виробничої мережі, з усіма даними, що зберігаються на ньому. Залишаються колишніми паролі, при віддаленому доступі вони продовжують передаватися у відкритому вигляді. Це погано навіть в межах захищеної мережі організації; в об'єднаній мережі виставки - це занадто суворе випробування чесності всіх учасників.

Ще один приклад зміни, про який часто забувають, - зберігання даних на резервних носіях. Для захисту даних на основних носіях застосовуються розвинені системи управління доступом; копії же нерідко просто лежать у шафах і отримати доступ до них можуть багато [13].

Перехоплення даних - дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються по багатьох каналах, їх захист може виявитися досить складним і дорогим. Технічні засоби перехоплення добре опрацьовані, доступні, прості в експлуатації, а встановити їх, наприклад, на кабельну мережу, може хто-завгодно, так що цю загрозу потрібно брати до уваги по відношенню не тільки до зовнішніх, але і до внутрішніх комунікацій.

Крадіжки обладнання є загрозою не лише для резервних носіїв, але і для комп'ютерів, особливо портативних. Часто ноутбуки залишають без нагляду на роботі або в автомобілі, іноді просто втрачають.

Небезпечною нетехнічною загрозою конфіденційності є методи морально-психологічного впливу, такі як «маскарад» - виконання дій під виглядом особи, яка володіє повноваженнями для доступу до даних.

До загроз, від яких важко захищатися, можна віднести зловживання повноваженнями. На багатьох типах систем привілейований користувач (наприклад системний адміністратор) здатний прочитати будь-який (незашифрований) файл, отримати доступ до пошти будь-якого користувача

тощо. Інший приклад - нанесення збитку при сервісному обслуговуванні. Зазвичай сервісний інженер одержує необмежений доступ до устаткування і має можливість діяти в обхід програмних захисних механізмів.

Такі основні загрози, які завдають найбільшої шкоди суб'єктам інформаційних відносин [36].

Правовідносини, що виникають у зв’язку із необхідністю забезпечувати безпеку інформаційних систем, найкраще врегульовані законодавством США. Ключову роль відіграє американський «Закон про інформаційну безпеку». Його мета - реалізація мінімально достатніх дій по забезпеченню безпеки інформації в федеральних комп'ютерних системах, без обмежень всього спектру можливих дій.

Характерно, що вже на початку Закону називається конкретний виконавець - Національний інститут стандартів і технологій (NIST), відповідальний за випуск стандартів та настанов, спрямованих на захист від знищення і несанкціонованого доступу до інформації, а також від крадіжок і підробок, виконуваних за допомогою комп'ютерів. Таким чином, мається на увазі як регламентація дій фахівців, так і підвищення інформованості всього суспільства.

Згідно Закону, всі оператори федеральних інформаційних систем, які містять конфіденційну інформацію, повинні сформувати плани забезпечення інформаційної безпеки. Обов'язковим є і періодичне навчання всього персоналу таких інформаційних систем. NIST, у свою чергу, зобов'язаний проводити дослідження природи і масштабу вразливих місць, виробляти економічно виправдані заходи захисту. Результати досліджень розраховані на застосування не тільки в державних системах, але і в приватному секторі.

Закон зобов'язує NIST координувати свою діяльність з іншими міністерствами і відомствами, включаючи Міністерство оборони, Міністерство енергетики, Агентство національної безпеки (ANS) та інші, щоб уникнути дублювання і несумісності.

Крім регламентації додаткових функцій NIST, Закон наказує створити при Міністерстві торгівлі комісію з інформаційної безпеки, яка повинна:

— виявляти перспективні управлінські, технічні, адміністративні та фізичні заходи, що сприяють підвищенню ІБ;

— видавати рекомендації Національному інституту стандартів і технологій, доводити їх до відома всіх зацікавлених відомств.

З практичної точки зору важливий розділ 6 Закону, що зобов'язує всі урядові відомства сформувати план забезпечення інформаційної безпеки, спрямований на те, щоб компенсувати ризики і запобігти можливий збиток від втрати, неправильного використання, несанкціонованого доступу або модифікації інформації у федеральних системах. Копії плану направляються в NIST і ANS [4].

У 1997 році з'явилося продовження описаного закону - закон "Про вдосконалення інформаційної безпеки", спрямований на посилення ролі Національного інституту стандартів і технологій та спрощення операцій з крипто-засобами. У законі констатується, що приватний сектор готовий надати крипто-засоби для забезпечення конфіденційності і цілісності (в тому числі автентичності) даних, що розробка і використання шифрувальних технологій повинні відбуватися на підставі вимог ринку, а не розпоряджень уряду. Крім того, тут наголошується, що за межами США є зіставні і загальнодоступні криптографічні технології, і це слід враховувати при виробленні експортних обмежень, щоб не знижувати конкурентоспроможність американських виробників апаратного і програмного забезпечення.

Для захисту федеральних інформаційних систем рекомендується більш широко застосовувати технологічні рішення, засновані на розробках приватного сектора. Крім того, пропонується оцінити можливості загальнодоступних зарубіжних розробок.

Вітається розробка правил безпеки, нейтральних по відношенню до конкретних технічних рішень, використання у федеральних ІС комерційних продуктів, участь у реалізації шифрувальних технологій, що дозволяє в

остаточному підсумку сформувати інфраструктуру, яку можна розглядати як резервну для федеральних інформаційних систем.

Важливо, що у відповідності з розділами 10 і далі передбачається виділення конкретних (і немалих) сум, називаються точні терміни реалізації програм партнерства та проведення досліджень інфраструктури з відкритими ключами, національної інфраструктури цифрових підписів. Зокрема, передбачається, що для центрів, які виготовляють електронні цифрові підписи,повинні бути розроблені типові правила і процедури, порядок ліцензування, стандарти аудиту [9].

У 2001 році був схвалений Палатою представників і переданий в Сенат новий варіант розглянутого законопроекту – Computer Security Enhancement Actof 2001 (HR 1259 RFS). У цьому варіанті примітно як те, що, в порівнянні з попередньою редакцією, було прибрано, так і те, що додалося.

За чотири роки (1997-2001 рр..) на законодавчому та інших рівнях інформаційної безпеки США було зроблено багато. Пом'якшені експортні обмеження на криптозасоби (у січні 2000 р.). Сформована інфраструктура з відкритими ключами. Розроблено велику кількість стандартів (наприклад, новий стандарт електронного цифрового підпису - FIPS 186-2, січень 2000 р.). Все це дозволило не загострювати більш уваги на криптографії як такої, а зосередитися на одному з її найважливіших додатків - аутентифікації, розглядаючи її за відпрацьованою на криптозасобах методикою. Очевидно, що, незалежно від долі законопроекту, в США буде сформована національна інфраструктура електронної аутентифікації. В даному випадку законотворча діяльність йде в ногу з прогресом інформаційних технологій [7].

Програма безпеки, що передбачає економічно виправдані захисні заходи і синхронізована з життєвим циклом ІС, згадується в законодавстві США неодноразово. Згідно з пунктом 3 534 ("Обов'язки федеральних відомств") глави II ("Інформаційна безпека") глави 35 ("Координація федеральної інформаційної політики") рубрики 44 ("Громадські видання і документи"), така програма повинна включати:

— періодичну оцінку ризиків з розглядом внутрішніх і зовнішніх загроз цілісності, конфіденційності та доступності систем, а також даних, асоційованих з критично важливими операціями і ресурсами;

— правила і процедури, що дозволяють, спираючись на проведений аналіз ризиків, економічно виправданим чином зменшити ризики до прийнятного рівня;

— навчання персоналу з метою інформування про існуючі ризики і про обов'язки, виконання яких необхідне для їх (ризиків) нейтралізації;

— періодичну перевірку і (пере) оцінку ефективності правил і процедур;

— дії при внесенні суттєвих змін в систему;

— процедури виявлення порушень інформаційної безпеки та реагування на них; ці процедури повинні допомогти зменшити ризики, уникнути великих втрат; організувати взаємодію з правоохоронними органами.

Звичайно, в законодавстві США є в достатній кількості і положення обмежувальної спрямованості, і директиви, які захищають інтереси таких відомств, як Міністерство оборони, ANS, але ми не будемо на них зупинятися.

З законодавстві Великобританії згадаємо сімейство так званих добровільних стандартів BS 7799, що допомагають організаціям на практиці сформувати програми безпеки [4].

1.3 Загальні відомості про ризики та управління ними

Управління ризиками розглядається нами на адміністративному рівні інформаційної безпеки, оскільки тільки керівництво організації здатне виділити необхідні ресурси, ініціювати і контролювати виконання відповідних програм.

Взагалі кажучи, управління ризиками, так само як і вироблення власної політики безпеки, актуально тільки для тих організацій, інформаційні системи яких або оброблювані дані можна вважати нестандартними. Звичайну організацію цілком влаштує типовий набір захисних заходів, вибраний на основі уявлення про типових ризики або взагалі без жодного аналізу ризиків Можна провести аналогію між індивідуальним будівництвом і отриманням квартири в районі масової забудови. У першому випадку необхідно прийняти безліч рішень,

оформити велику кількість паперів, у другому досить визначитися лише з декількома параметрами.

Використання інформаційних систем пов'язане з певною сукупністю ризиків. Коли можливий збиток неприйнятно великий, необхідно вжити економічно виправдані заходи захисту. Періодична переоцінка ризиків необхідна для контролю ефективності діяльності в галузі безпеки і для врахування змін обстановки.

З кількісної точки зору рівень ризику є функцією вірогідності реалізації певної загрози (що використовує деякі вразливі місця), а також величини можливого збитку.

Таким чином, суть заходів щодо управління ризиками полягає в тому, щоб оцінити їх розмір, виробити ефективні і економічні заходи зниження ризиків, а потім переконатися, що ризики поміщені в прийнятні рамки (і залишаються такими). Отже, управління ризиками включає в себе два види діяльності, які чергуються циклічно:

— вимірювання ризиків;
— вибір ефективних і економічних захисних засобів (нейтралізація ризиків).
— По відношенню до виявлених ризиків можливі наступні дії:
— ліквідація ризику (наприклад, за рахунок усунення причини);
— зменшення ризику (наприклад, за рахунок використання додаткових захисних засобів);
— прийняття ризику (і вироблення плану дії у відповідних умовах);
— переадресація ризику (наприклад, шляхом укладення страхової угоди).

Процес управління ризиками можна розділити на наступні етапи:

— Вибір аналізованих об'єктів і рівня деталізації їх розгляду.
— Вибір методології оцінки ризиків.
— Ідентифікація активів.
— Аналіз загроз і їх наслідків, виявлення вразливих місць в захисті.
— Оцінка ризиків.
— Вибір захисних заходів.

— Реалізація та перевірка вибраних заходів.

— Оцінка залишкового ризику [36].

Етапи 6 і 7 відносяться до вибору і впровадження захисних засобів (нейтралізації ризиків), решта - до оцінки ризиків.

Вже перерахування етапів показує, що управління ризиками - процес циклічний. По суті, останній етап - це оператор кінця циклу, що приписує повернутися до початку. Ризики потрібно контролювати постійно, періодично проводячи їх переоцінку. Відзначимо, що сумлінно виконана і ретельно документована перша оцінка може істотно спростити подальшу діяльність.

Управління ризиками, як і будь-яку іншу діяльність в області інформаційної безпеки, необхідно інтегрувати в життєвий цикл інформаційних систем. Тоді ефект виявляється найбільшим, а витрати - мінімальними. Раніше ми визначили п'ять етапів життєвого циклу. Коротко опишемо, що може дати управління ризиками на кожному з них [13].

На етапі ініціації відомі ризики слід врахувати при виробленні вимог до системи взагалі і засобам безпеки зокрема. На етапі закупівлі (розробки) знання ризиків допоможе вибрати відповідні архітектурні рішення, які грають ключову роль в забезпеченні безпеки. На етапі установки виявлені ризики слід враховувати при конфігуруванні, тестуванні та перевірці раніше сформульованих вимог, а повний цикл управління ризиками повинен передувати впровадженню системи в експлуатацію.На етапі експлуатації управління ризиками повинне супроводжувати всі істотні зміни в системі.

При виведенні системи з експлуатації управління ризиками допомагає переконатися в тому, що міграція даних відбувається безпечним чином.

Вибір аналізованих об'єктів і рівня деталізації їх розгляду - перший крок в оцінці ризиків. Для невеликої організації допустимо розглядати всю інформаційну інфраструктуру; проте якщо організація крупна, всеосяжна оцінка може вимагати неприйнятних витрат часу і сил. У такому разі слід зосередитися на найбільш важливих сервісах, заздалегідь погоджуючись з наближеністю

підсумкової оцінки. Якщо важливих сервісів все ще багато, вибираються ті з них, ризики для яких свідомо великі або невідомі [36].

Ми вже вказували на доцільність створення карти інформаційної системи організації. Для управління ризиками подібна карта особливо важлива, оскільки вона наочно показує, які сервіси вибрані для аналізу, а якими довелося знехтувати. Якщо інформаційна система міняється, а карта підтримується в актуальному стані, то при переоцінці ризиків відразу стане ясно, які нові або істотно змінилися сервіси потребують розгляду.

Взагалі кажучи, уразливим є кожен компонент інформаційної системи - від мережевого кабелю, який можуть прогризти миші, до бази даних, яка може бути зруйнована через невмілих дій адміністратора. Як правило, в сферу аналізу неможливо включити кожен гвинтик і кожен байт. Доводиться зупинятися на деякому рівні деталізації, знову-таки віддаючи собі звіт в наближеності оцінки. Для нових систем переважний детальний аналіз; стара система, що піддалася невеликим модифікаціям, може бути проаналізована більш поверхнево [47].

Дуже важливо вибрати розумну методологію оцінки ризиків. Метою оцінки є одержання відповіді на два питання: прийнятні чи існуючі ризики, і якщо ні, то які захисні засоби варто використовувати. Значить, оцінка повинна бути кількісною, що допускає зіставлення із заздалегідь вибраними межами допустимості і витратами на реалізацію нових регуляторів безпеки. Управління ризиками - типова оптимізаційна задача, і існує досить багато програмних продуктів, здатних допомогти в її вирішенні (іноді подібні продукти просто додаються до книг з інформаційної безпеки). Принципова трудність, проте, полягає в неточності початкових даних. Можна, звичайно, спробувати отримати для всіх аналізованих величин грошовий вираз, вирахувати все з точністю до копійки, але великого сенсу в цьому немає. Практичніше користуватися умовними одиницями. У найпростішому і цілком допустимому випадку можна користуватися трибальною шкалою. Далі ми продемонструємо, як це робиться.

При ідентифікації активів, тобто тих ресурсів і цінностей, які організація намагається захистити, слід, звичайно, враховувати не тільки компоненти

інформаційної системи, але і підтримуючу інфраструктуру, персонал, а також нематеріальні цінності, такі як репутація організації. Відправною точкою тут є уявлення про місію організації, тобто про основні напрямки діяльності, які бажано (або необхідно) зберегти в будь-якому випадку. Слід в першу чергу описати зовнішній інтерфейс організації, що розглядається як абстрактний об'єкт.

Одним з головних результатів процесу ідентифікації активів є отримання детальної інформаційної структури організації та способів її (структури) використання. Ці відомості доцільно нанести на карту інформаційної системи як грані відповідних об'єктів.

Інформаційною основою скільки-небудь крупної організації є мережа, тому в число апаратних активів слід включити комп'ютери (сервери, робочі станції, ПК), периферійні пристрої, зовнішні інтерфейси, кабельне господарство, активне мережеве обладнання (мости, маршрутизатори тощо). До програмних активів, ймовірно, будуть віднесені операційні системи (мережева, серверні і клієнтські), прикладне програмне забезпечення, інструментальні засоби, засоби управління мережею і окремими системами. Важливо зафіксувати, де (у яких вузлах мережі) зберігається програмне забезпечення, і з яких вузлів воно використовується. Третім видом інформаційних активів є дані, які зберігаються, обробляються і передаються по мережі. Слід класифікувати дані по типах і ступеню конфіденційності, виявити місця їх зберігання і обробки, способи доступу до них. Все це важливо для оцінки наслідків порушень інформаційної безпеки [36].

Управління ризиками - процес далеко не лінійний. Практично всі його етапи пов'язані між собою, і по завершенні майже будь-якого з них може виникнути необхідність повернення до попереднього. Так, при ідентифікації активів може виявитися, що вибрані межі аналізу слід розширити, а ступінь деталізації - збільшити. Особливо важкий первинний аналіз, коли багатократні повернення до початку неминучі.

Етапи, попередні аналізу загроз, можна вважати підготовчими, оскільки, строго кажучи, вони безпосередньо з ризиками не пов'язані. Ризик з'являється там, де є загрози.

Короткий перелік найбільш поширених загроз був розглянутий нами раніше. На жаль, на практиці загроз значно більше, причому далеко не всі з них носять комп'ютерний характер. Перший крок в аналізі загроз - їх ідентифікація. Розглянуті види загроз слід вибирати виходячи з міркувань здорового глузду (виключивши, наприклад, землетруси, проте не забуваючи про можливість захоплення організації терористами), але в межах обраних видів провести максимально докладний аналіз [26].

Доцільно виявляти не тільки самі загрози, але і джерела їх виникнення - це допоможе у виборі додаткових засобів захисту. Наприклад, нелегальний вхід в систему може стати наслідком відтворення початкового діалогу, підбору пароля або підключення до мережі неавторизованого устаткування. Очевидно, для протидії кожному з перерахованих способів нелегального входу потрібні свої механізми безпеки.

Після ідентифікації загрози необхідно оцінити ймовірність її здійснення. Допустимо використовувати при цьому трибальною шкалою (низька (1), середня (2) і висока (3) ймовірність).

Крім імовірності здійснення, важливий розмір потенційного збитку. Наприклад, пожежі бувають нечасто, але збиток від кожного з них, як правило, великий. Оцінюючи розмір шкоди, необхідно мати на увазі не тільки безпосередні витрати на заміну устаткування або відновлення інформації, але й більш віддалені, такі як підрив репутації, ослаблення позицій на ринку і т.п.

Після того, як накопичені вихідні дані та оцінено ступінь невизначеності, можна переходити до обробки інформації, тобто власне до оцінки ризиків. Цілком допустимо застосувати такий простий метод, як множення вірогідності здійснення загрози на передбачуваний збиток. Якщо для вірогідності і збитку використовувати трибальною шкалою, то можливих добутків буде шість: 1, 2, 3, 4, 6 і 9. Перші два результату можна віднести до низького ризику, третій і

четвертий - до середнього, два останніх - до високого, після чого з'являється можливість знову привести їх до трибальною шкалою. За цією шкалою і слід оцінювати прийнятність ризиків. Правда, граничні випадки, коли обчислена величина співпала з прийнятною, доцільно розглядати більш ретельно через наближеного характеру результату [36].

Якщо будь-які ризики виявилися неприпустимо високими, необхідно їх нейтралізувати, реалізувавши додаткові заходи захисту. Як правило, для ліквідації або нейтралізації вразливого місця, що зробив загрозу реальною, існує декілька механізмів безпеки, різних по ефективності і вартості. Наприклад, якщо велика ймовірність нелегального входу в систему, можна зажадати, щоб користувачі вибирали довгі паролі (скажімо, не менше восьми символів), задіяти програму генерації паролів або закупити інтегровану систему аутентифікації на основі інтелектуальних карт. Якщо є ймовірність умисного пошкодження сервера баз даних, що може мати серйозні наслідки, можна врізати замок у двері серверної кімнати або поставити біля кожного сервера по охоронцеві.

Оцінюючи вартість заходів захисту, доводиться, зрозуміло, враховувати не тільки прямі витрати на закупівлю обладнання або програм, але і витрати на впровадження новинки і, зокрема, навчання і перепідготовку персоналу. Цю вартість також можна оцінити за трибальною шкалою і потім зіставити її з різницею між обчисленим і допустимим ризиком. Якщо за цим показником новий засіб виявляється економічно вигідним, його можна взяти на замітку (відповідних засобів, ймовірно, буде декілька). Однак якщо засіб виявиться дорогим, його не слід відразу відкидати, пам'ятаючи про наближеність розрахунків.

Вибираючи відповідний спосіб захисту, доцільно враховувати можливість екранування одним механізмом забезпечення безпеки відразу декількох прикладних сервісів. Так вчинили в Массачусетському технологічному інституті, захистивши декілька тисяч комп'ютерів сервером аутентифікації Kerberos [9].

Важливою обставиною є сумісність нового засобу зі сформованою організаційною і апаратно-програмної структурою, з традиціями організації. Заходи безпеки, як правило, носять недружній характер, що може негативно позначитися на ентузіазмі працівників.

Можна уявити собі ситуацію, коли для нейтралізації ризику не існує ефективних і прийнятних за ціною заходів. Наприклад, компанія, що базується в сейсмічно небезпечній зоні, не завжди може дозволити собі будівництво захищеної штаб-квартири. У такому випадку доводиться піднімати планку прийнятного ризику і переносити центр ваги на пом'якшення наслідків і вироблення планів відновлення після аварій, стихійних лих та інших подій. Продовжуючи приклад з сейсмонебезпечних, можна рекомендувати регулярне тиражування даних в інше місто і оволодіння засобами відновлення первинної бази даних [4].

Як і всяку іншу діяльність, реалізацію і перевірку нових регуляторів безпеки слід попередньо планувати. У плані необхідно врахувати наявність фінансових засобів і терміни навчання персоналу. Якщо мова йде про програмно-технічному механізмі захисту, потрібно скласти план тестування (автономного і комплексного).

Коли намічені заходи прийняті, необхідно перевірити їх дієвість, тобто переконатися, що залишкові ризики стали прийнятними. Якщо це насправді так, значить, можна спокійно намічати дату найближчої переоцінки [36].

2. СТРУКТУРА ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА, РИЗИКИ ТА ЗАГРОЗИ

2.1 Інформаційні системи та кібербезпека крізь призму системного підходу до управління бізнесом

Технологічний прогрес, який із новою силою вибухнув наприкінці двадцятого, і особливо – у двадцять першому столітті, логічно обумовлює зміни у стратегіях і методах ведення бізнесу, визначає нові напрямки організаційного і технічного супроводу господарської діяльності. Використання новітніх інформаційних технологій та інформаційних систем має комплексний вплив практично на всі сфери функціонування бізнесу. Завдяки інформаційним технологіям оптимізується виробництво, підвищується ефективність менеджменту, прискорюються процеси прийняття рішень, здійснюється контроль над використанням ресурсів. Використання інформаційних технологій уможливлює динамічну комунікацію між структурними одиницями бізнесу, що особливо актуально для суб’єктів, підприємницька діяльність яких охоплює декілька регіонів. Загалом, невпинний стрімкий розвитокінформаційних технологій створює передумови для здобуття конкурентних переваг тими суб’єктами господарювання, які тримають руку на пульсі усіх інновацій[44].

Розвиток інтернету, програмного забезпечення, еволюція технічних засобів сприяють появі нових сервісів та послуг для бізнесу. Використання інформаційних технологій у підприємницькій діяльності вже давно вийшло за межі внутрішніх процесів та стало необхідним методом взаємодії із клієнтами. Із застосуванням інформаційних технологій здійснюється просування на ринку, пошук клієнтів, часто налагоджується договірна співпраця, інформаційних технологій спрощують здійснення розрахунків. По суті, інформаційні технології ліквідують левову частку територіальних обмежень для ведення бізнесу, окрім логістичних, митних та деяких інших. Підприємство, незалежно від свого місця розташування, масштабів діяльності, має змогу продавати свої товари і послуги, залучати співробітників на дистанційній основі тощо.

Особливо важливою є роль інформаційних технологій у сфері маркетингу. При цьому ідеться про двосторонню взаємодію: донесення до аудиторії відомостей про пропозицію, – з одного боку, – і дослідження попиту, – з іншого. Щодо попиту, то новітні інформаційні технології надають підприємствам багатий інструментарій не тільки для його дослідження, але і для формування. Уміле використання відповідних інформаційно-технічних засобів, систем, методів дозволяє підприємству ефективно пропонувати на ринку нові, у тому числі неіснуючі раніше, товари і послуги.

В цілому, на сьогодні інформаційні технології активно використовуються у веденні бізнесу для наступних цілей:

— автоматизація, оптимізація виробничих процесів, управління ними;
— створення високих ергономічних показників задля максимального використання людського ресурсу;
— структурна та міжособистісна комунікація, управління персоналом;
— ведення бухгалтерського обліку і звітності;
— маркетингові дослідження, просування на ринку;
— пошук та обробка необхідної для прийняття рішень інформації;
— перемовини і налагодження співпраці із клієнтом (покупцем, замовником тощо);
— контроль за бізнес-процесами [59].

Наведений перелік, однозначно, не є вичерпним. Окрім того, кожен запропонований вище пункт є збірним та може бути розділений на окремі взаємопов’язані елементи. Їхня кількість і зміст у кожному випадку залежать від галузі (сфери, ніші), організаційно-правової форми, юрисдикції, масштабів діяльності конкретного суб’єкта господарювання тощо. Проте, очевидно, що на сьогодні інформаційні технології пронизують увесь спектр бізнес-процесів, а використання інформаційних технологій є об’єктивною необхідністю практично для кожного підприємства.

З огляду на це, виняткової актуальності набуває питання забезпечення безпеки підприємства при використанні інформаційних технологій. Комплексний характер проблеми вимагає і комплексного підходу до її

вирішення: так, рівень інформаційної безпеки підприємства значною мірою залежить від його структурних, управлінських, фінансових, матеріально-технічних особливостей тощо [46].

Виняткову роль у забезпеченні кібербезпеки бізнесу відіграє менеджмент. У цьому контексті варто звернути особливу увагу на системний підхід до управління, який активно розвинувся наприкінці минулого століття і досі залишається одним із основних у теорії і практиці менеджменту. Центральною категорією системного підходу є бізнес-процеси. По суті, управління підприємством зводиться до їхньої гармонізації та вдосконалення.

Бізнес-процес класифікують за низкою ознак. Ми розглянемо лише окремі класифікаційні системи, найбільш важливі для осмислення теми цього дослідження. Так, за значенням для функціонування бізнесу процеси поділяються на такі види:

— стратегічні;
— основні робочі процеси;
— допоміжні робочі процеси.

Стратегічні процеси, на відміну від робочих, не передбачають вирішення конкретних завдань, а спрямовані на визначення місії, принципів, довгострокових цілей підприємства тощо [21].

За сферою впливу бізнес-процеси класифікуються наступним чином:

— однофункціональні;
— міжфункціональні.

До першої групи належать найпростіші процеси, які переважно потребують залучення мінімальних, чітко визначених ресурсів (людських, інформаційних, матеріальних тощо). Однофункціональні процеси зазвичай закріплені за конкретною структурною одиницею та спрямовані на втілення простого (не розділеного на частини) завдання [36].

Міжфункціональні процеси, у свою чергу, найчастіше передбачають участь (взаємодію) декількох структурних одиниць, є довготривалими у часі (або ж триваючими), потребують залучення значного обсягу ресурсів різного виду.

Міжфункціональні процеси зазвичай можна логічно поділити на окремі етапи, частини тощо. Класичними прикладами міжфункціональних процесів є виробництво, взаємодія з клієнтом та інші.

Осмислення міжфункціональних процесів, які відбуваються на підприємстві, має безпосереднє значення для забезпечення інформаційної безпеки із двох причин. По-перше, саме міжфункціональні процеси, з огляду на їхню масштабність, передусім потребують інформаційно-технологічного супроводу. Складність процесів логічно обумовлює складність інформаційних систем, які використовуються для оптимізації. По-друге, інформаційно-технічне обслуговування бізнесу в цілому і кібербезпека зокрема самі по собі є міжфункціональними процесами [56].

У межах системного підходу до управління підприємством революційним способом на сьогодні вважається реінжиніринг бізнес-процесів. Найвагоміший внесок у розробку цього методичного напрямку зробили М. Хаммер і Дж. Чампі. Реінжиніринг, за визначенням цих авторів, полягає у кардинальному перепроектуванні бізнес-процесів задля досягнення вагомих покращень у всіх ключових сферах діяльності підприємства, серед яких і економічна, у тому числі інформаційна, безпека.

Упровадження реінжинірингу завжди включає економічний, організаційний та технологічний аспект. При цьому одним із засадничих принципів реінжинірингу є зосередження передусім не на напрямках (функціях), а на процесах, які відбуваються на підприємстві (що, загалом, властиво і системному підходу в цілому). Відповідно, саме бізнес-процеси визначаються основним об’єктом менеджерського впливу. Оптимізація процесів, у свою чергу, сприяє максимально ефективному і ощадливому використанню ресурсів, а також злагодженій взаємодії між структурними одиницями підприємства [63].

В умовах сьогодення успішний реінжиніринг бізнес-процесів практично неможливо втілити без застосування інформаційних технологій. Левова частка впливу інформаційних технологій на процеси підприємства зводиться до їхньої

автоматизації. Остання, всупереч поширеному уявленню, стосується не тільки виробництва, але і сфери обліку та звітності, комунікації, логістики тощо [23].

Реінжиніринг бізнес-процесів є одним із ключових управлінських методів, придатних для превенції кіберзагроз у діяльності підприємства. Під кіберзагрозами розуміються будь-які обставини (події), а також діяння людей, які можуть завдати збитків автоматизованим системам та безпеці інформації (відповідно до обраної політики). Умисні спроби реалізації кіберзагроз, незалежно від їхньої успішності, називають кібератаками.

Практика підприємницької діяльності в Україні свідчить про існування істотного розриву між застосуванням інформаційних технологій, інформаційних систем у бізнесі і вжиттям заходів для забезпечення інформаційної безпеки. Якщо перше у вітчизняному бізнес-середовищі вже давно сприймається як само собою зрозуміле та необхідне, то ризики кібербезпеки багатьма підприємцями недооцінюються, а то і цілком ігноруються. Майже весь сегмент малого і левова частка середнього бізнесу в Україні на старті своєї діяльності або взагалі не розглядають безпеку інформаційних систем як окремий процес і напрямок, який потребує комплексного управлінського і ресурсного забезпечення, або ж уживають заходів для забезпечення кібербезпеки дуже фрагментарно [14].

Приводом для перегляду безпекової політики підприємства (чи її відсутності) у частині кібербезпеки дуже часто стає реалізація кіберзагроз, іноді неодноразова. З точки зору класифікації бізнес-процесів, описаної вище, безпека інформаційних систем зазвичай є міжфункціональним допоміжним робочим процесом підприємства. Очевидно, саме допоміжний характер цього процесу, його своєрідний фоновий режим дозволяє деякий час не помічати або ж недооцінювати кібербезпеку як елемент збірного поняття економічної безпеки. Водночас, з огляду на міжфункціональність процесу забезпечення інформаційної безпеки, його запровадження вже у ході роботи підприємства передбачає зміни практично у всіх без винятку інших процесах. Саме реінжиніринг бізнес-процесів надає для цього необхідний управлінський інструментарій [31].

2.2 Структурний аналіз інформаційного середовища та загальна характеристика ризиків кібербезпеки підприємства

Інформаційне середовище підприємства формують інформаційні системи та користувачі.

Інформаційні системи складаються із трьох основних елементів:

— устаткування;
— програмне забезпечення;
— дані.

До устаткування, зокрема, належать:

— сервери;
— мережеві пристрої;
— пристрої для зберігання даних;
— комп’ютерні термінали;
— інше спеціалізоване обладнання.

В цілому, до устаткування відноситься комп’ютерне та інше обладнання, телекомунікаційні кабелі, приміщення тощо. Устаткування є речовим вираженням інформаційної системи [36].

Програмне забезпечення складається із таких частин:

— операційна система;
— система управління, аналізу та обробки баз даних;
— антивірусне програмне забезпечення.

Під операційною системою прийнято розуміти базовий комплекс програм, що виконує управління апаратною складовою комп'ютера або віртуальної машини, забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем [65].

У операційній системі відбуваються такі види процесів:

— експлуатаційні;
— робочі;
— обслуговуючі;
— пов’язані із розвитком.

Експлуатаційні процеси становлять левову частку процесів операційної системи. До них відносяться найпоширеніші, «рутинні», повторювані процеси, які, водночас, не вимагають особливої користувацької компетентності. Робочі процеси забезпечують постійну підтримку користувачів, діагностику і моніторинг інформаційної системи в цілому. Обслуговуючі процеси покликані забезпечити доступність, продуктивність і безперервність функціонування інформаційної системи у середньостроковій і довготривалій перспективі. Процеси, пов'язані із розвитком, – це ті, у межах яких відбувається планування змін у інформаційній системі, генерування та запровадження нових рішень.

Система управління, аналізу, та обробки баз даних визначається як набір взаємопов'язаних даних (баз даних) та програм доступу до них. Через систему управління базами даних забезпечується можливість створення, збору, збереження, оновлення інформації та обміну нею, контролю доступу до даних [67].

Додатки є програмним забезпеченням, яке використовується з метою обробки даних відповідно до потреб, представлення даних у необхідній формі тощо. Додатки, які використовуються у інформаційно-технологічному супроводі підприємницької діяльності, можна класифікувати за їхніми функціями, тобто напрямками (сферами, завданнями) впливу на функціонування бізнесу. Зокрема, додатки можуть стосуватися:

— планування ресурсів підприємства;
— бухгалтерського обліку і фінансової звітності;
— взаємодії з клієнтами;
— логістики;
— виробництва;
— управління персоналом тощо [35].

Як бачимо, додатки інтегровані практично з усіма бізнес-процесами. Застосування додатків сприяє гармонізації процесів, які відбуваються на підприємстві, підвищенню їхньої ефективності.

Під даними у інформатиці розуміють інформацію, подану у формалізованому вигляді, придатному для обробки (інтерпретації) автоматичними засобами за можливої участі людини [12].

Наступним елементом інформаційного середовища підприємства є користувачі. Користувачі класифікуються за рівнем (сферою) доступу до складових інформаційної системи. Так, левова частка користувачів у межах підприємства переважно безпосередньо використовує додатки та опосередковано взаємодіє із системою управління базами даних (наприклад, при створенні чи поширенні інформації). Тільки окремі користувачі наділяються доступом до операційної системи [33].

За характером взаємодії (взаємовідношення) із конкретним підприємством серед користувачів інформаційної системи підприємства можна виділити:

— власників;
— працівників;
— осіб, які надають послуги підприємству (на цивільно-правовій основі, періодично або за необхідності);
— клієнтів підприємства (покупців, замовників тощо);
— партнерів підприємства (контрагентів, з якими підприємство співпрацює на договірній основі).

Запропонований перелік не претендує на вичерпність та включає лише найбільш розповсюджені, універсальні групи користувачів інформаційної системи підприємства за звичайних обставин [30].

Окрім вже наведеної класифікації, доцільно також розрізняти користувачів інформаційної системи підприємства за фактором легальності їхнього доступу до ІС (як в цілому, так і щодо окремих елементів). Відповідно, користувачі можуть бути:

— санкціонованими;
— несанкціонованими [50].

Саме у контексті взаємозв’язку окремих елементів інформаційної системи підприємства між собою, а також взаємодії користувачів з інформаційною системою підприємства (чи окремими її складовими) доцільно говорити про кібербезпеку, або ж безпеку інформаційної системи у межах конкретного бізнесу. Під останньою прийнято розуміти стан захищеності устаткування, програмного забезпечення і, власне, даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, можливість її використання для визначених цілей [41].

У свою чергу, забезпечення кібербезпеки передбачає:

— запобігання внутрішньо-системних ризиків інформаційної системи;
— запобігання негативного впливу зовнішнього середовища на функціонування інформаційної системи;
— запобігання шкідливого впливу людей і зокрема, користувачів [22].

Під внутрішньо-системними ризиками маються на увазі порушення функціонування інформаційної системи, обумовлені недосконалостями самої інформаційної системи, без будь-якого зовнішнього впливу. Серед цієї категорії ризиків окремо можна виділити збої, тобто порушення нормального функціонування інформаційної системи в цілому чи окремих її складових, і окремо – загрози для цілісності, конфіденційності, доступності та/або можливості цільового використання інформації, які існують при нормальній роботі інформаційної системи або її елементів [40].

Суттєво, що відсутність зовнішнього впливу у контексті внутрішньо-системних ризиків інформаційної системи є доволі умовною характеристикою. Так, будь-яка інформаційна система (чи окремий її елемент) має свого розробника, а відтак, саме його помилкою або недалекоглядністю часто обумовлені системні збої, а тим більше, не пов’язані зі збоями внутрішньо-системні загрози.

Під негативним впливом зовнішнього середовища як фактором ризику для кібербезпеки підприємства маються на увазі чинники, які безпосередньо не пов’язані ані з функціонуванням інформаційної системи самим по собі, ані з

взаємодією користувачів з інформаційної системи. Зокрема, ідеться про цілісність і справність устаткування, безпеку приміщень, у яких воно знаходиться, тощо. Перелік чинників ризику у цьому контексті необмежений: відповідні чинники можуть мати метеорологічний, геологічний, астрономічний, механічний, зоологічний, електричний та інший характер [24].

Шкідливий вплив людей на функціонування інформаційної системи підприємства може бути вчинений як умисними, так і необережними діями чи бездіяльністю. При цьому умисел може стосуватися як безпосередньо реалізації ризиків кібербезпеки, так і заподіяння підприємству шкоди іншого характеру. Наприклад, крадіжка устаткування (у розумінні – елемента інформаційної системи) підприємства для його продажу (з корисливою метою) хоч і не здійснюється з наміром порушення цілісності, конфіденційності, доступності та/або можливості цільового використання інформації, проте призводить до відповідних наслідків. При цьому люди, які здійснюють шкідливий впливу на функціонування інформаційної системи, не є користувачами [37].

Також суттєво, що користувачами інформаційної системи можуть бути не лише люди, але і боти (програми), юридичні особи тощо. Проте усі неантропологічні користувачі інформаційної системи, врешті, все одно зводяться до людини чи групи людей [40].

Превенція внутрішньо-системних ризиків, негативного впливу зовнішнього середовища та шкідливих діянь людей і/зокрема користувачів є взаємопов’язаними заходами, здійснення яких необхідне для забезпечення інформаційної безпеки підприємства. Ефективність цих заходів можлива лише за умови їхнього комплексного застосування.

Реалізація ризиків кібербезпеки підприємства може мати наступні наслідки:

— витік інформації;
— втрата цілісності інформації;
— модифікація (зміна) інформації;
— втрата доступу інформації для санкціонованих користувачів тощо [38].

Усі ці наслідки є шкідливими для функціонування бізнесу в цілому. Так, наприклад, витік інформації передбачає порушення її режиму. Зокрема, ідеться про таємну, конфіденційну та службову інформацію, яка охороняється законом, іншими актами, у тому числі локальними (прийнятими та чинними в межах конкретного підприємства чи організації). Оприлюднення відповідної інформації може завдати шкоди законним інтересам, діловій репутації підприємства, а в окремих випадках навіть стати приводом для застосування до нього заходів юридичної відповідальності. Останнє можливо, наприклад, за умови протиправного розповсюдження персональних даних, володільцем чи розпорядником яких є підприємство, або ж таємної (комерційна таємниця) чи конфіденційної інформації контрагентів підприємства, яка стала відома у процесі договірної співпраці [66].

Втрата цілісності інформації спотворює базу для прийняття важливих для бізнесу рішень, а модифікація інформації може обумовити прийняття рішень, які в подальшому завдадуть шкоди підприємству. Недоступність інформації для санкціонованих користувачів унеможливлює злагоджене функціонування підприємства та послідовно гальмує, а то і перериває низку бізнес-процесів [42].

По суті, спектр загроз кібербезпеки підприємства розширюється пропорційно розвитку інформаційних технологій в цілому. Відповідно, з кожним днем з’являються нові ризики, часто дедалі витонченіші, тобто складніші для виявлення і протидії та масштабніші за наслідками реалізації.

Останнім часом у інформатиці та юриспруденції закріпилося поняття кіберзлочинності. Так, під кіберзлочинами розуміють правопорушення, у ході яких здійснюється викрадення, спотворення, знищення інформації, розміщеної у інформаційній системі. При цьому заподіяння шкоди інформаційній системі може бути як кінцевою метою вчинення злочину (суб’єктивною стороною злочину), так і способом досягнення іншої злочинної мети (об’єктивною стороною злочину). Найчастіше кіберзлочини вчиняються із корисливих, а також із хуліганських мотивів. Ці злочини називають також інформаційними [70].

Для прикладу, Інтерпол використовує таку класифікацію кіберзлочинів:

— несанкціонований доступ та перехоплення;
— ухилення від плати за користування (так звана крадіжка часу);
— комп'ютерний вірус;
— зміна комп'ютерних даних;
— шахрайство з банкоматами;
— комп'ютерне шахрайство;
— незаконне копіювання;
— телефонне шахрайство;
— комп'ютерний саботаж;
— комп'ютерна підробка та інші [57].

Конвенція Ради Європи по боротьбі з кіберзлочинністю, яка, до речі, ратифікована вищим законодавчим органом України, групує інформаційні злочини наступним чином:

— злочини проти конфіденційності, цілісності та доступності інформаційних систем (зокрема, даних);
— шахрайство та підробка, пов'язані із використанням комп'ютерів;
— злочини, пов'язані із протиправним розміщенням інформації у мережах (зокрема, протиправної інформації);
— злочини проти авторських та суміжних прав [36].

Кримінальний кодекс України визначає всього чотири різновиди складу злочину, безпосередньо пов'язаних із сферою безпеки інформаційних систем, зокрема:

— несанкціоноване втручання у роботу комп'ютерів, мереж, автоматизованих систем (ст. 361);
— створення та розповсюдження вірусів (ст. 361-1);
— зловживання правом доступу до інформації, яка обробляється у комп'ютерах, мережах, автоматизованих системах, під яким розуміється протиправне надання доступу до відповідної інформації стороннім особам (ст. 361-2);

— несанкціоновані дії з інформацією, яка обробляється у комп'ютерах, мережах, автоматизованих системах, вчинені особою, яка має право доступу до такої інформації (ст. 362) [16].

Зазначені діяння є саме кримінальними правопорушеннями за умови, якщо вони вчинені належним суб'єктом, а також за низки інших умов (наприклад, заподіяння шкоди відповідного характеру і обсягу). Зазначимо, що до інформаційних злочинів відносяться лише найнебезпечніші діяння у кіберпросторі, які не вичерпують усього спектру існуючих кіберзагроз [18].

В цілому, залежно від сфери (характеру) виникнення, загрози безпеки інформаційних систем поділяються на такі групи:

— природні;
— технічні;
— програмні (пов'язані із програмним забезпеченням);
— користувацькі [45].

Ця класифікація частково уже була розглянута вище у контексті напрямків превенції кіберзагроз підприємства. Прикладами природних загроз є повені, буревії, землетруси тощо. Їхнє значення як дестабілізуючих факторів кібербезпеки оцінюється з урахуванням повторюваності, частоти (за умови повторюваності) і рівня впливу (сили коливань, висоти води тощо). Ці показники варіюються залежно від розташування конкретного підприємства та. Меншою мірою, від інших чинників [49].

Технічні загрози кібербезпеки полягають у несправності чи пошкодженні устаткування (обладнання), яке є невід'ємною складовою інформаційній системі. Найчастіше технічні загрози мають механічний, електричний, термічний, рідше хімічний характер [58].

Варто зазначити, що класифікація загроз безпеки інформаційних систем залежно від сфери а також характеру їх виникнення є доволі умовною і, по суті, здійснюється за принципом першості впливу того чи іншого дестабілізуючого фактора. В подальшому, якщо реалізацію ризику не вдасться зупинити чи, принаймні, звести до мінімуму, вона обумовить ланцюгову реакцію. Так,

наприклад, така природна загроза, як повінь, може не лише тимчасово обмежити доступ до устаткування, але і спричинити короткі замикання, корозію тощо [60].

Програмні загрози кібербезпеки є найширшою групою, яка, з огляду на свою масштабність та динамічність, практично не піддається чіткому окресленню. Програмні загрози можуть бути пов’язані як із власним програмним забезпеченням інформаційної системи, так і з втручанням сторонніх програм.

Загрози, не пов’язані із втручанням сторонніх програм (вони ж – внутрішньо-системні), можуть існувати під час нормального функціонування програмного забезпечення вінформаційній системі (внаслідок умислу чи недалекоглядності, помилки розробника), а можуть бути пов’язаними із збоєм, тобто порушенням нормального функціонування. Докладніше про це вже ішлося вище.

Сторонні програми проникають у інформаційну систему та порушують доступність, цілісність, захищеність інформації, можливість її цільового використання. Для загального позначення більшості шкідливих сторонніх програм прийнято використовувати поняття вірусів. Прикладами (різновидами) вірусів, зокрема, є бутові (завантажувальні) віруси, хробаки, троянські коні, кейлогери, перезаписуючівірусита багато інших [69].

Користувацькі загрози безпеки інформаційних систем можна поділити на необережні діяння (наприклад, помилку) та умисні дії. Останні характеризуються чітким наміром особи щодо порушення конфіденційності, цілісності, доступності інформації та інших негативних наслідків для інформаційній системі [53].

Говорячи про запобігання ризикам кібербезпеки на конкретному підприємстві, необхідно з’ясувати уразливість його інформаційної системи до кіберзагроз. Уразливість інформаційної системи тлумачать як ознаку, яка характеризує наявність і масштабність (за наявності) недоліків та прогалин в устаткуванні і, перш за все, програмному забезпеченні інформаційної системи, а також супутніх обставин організаційного, управлінського, фізичного, антропогенного та іншого характеру, які можуть як окремо, так і в комплексі

обумовлювати реалізацію ризиків кібербезпеки або ж сприяти такій реалізації[48].

За критерієм уразливості інформаційної системи підприємства можуть визначатися як схильні або не схильні до загроз. Схильними до загроз є підприємства, інформаційні системи яких характеризуються високим рівнем уразливості, і навпаки. Суттєво, що показник уразливості об'єктивно не може бути нульовим, так як спектр кіберзагроз є занадто широким і мінливим. Відповідно, доречно говорити не про наявність або відсутність уразливості інформаційної системи, а про її допустиме або ж недопустиме значення [61].

Підвищення уразливості інформаційної системи може бути обумовлено численними факторами, які самі по собі не обов'язково є негативними. Такими факторами є, наприклад, висока стандартизація устаткування і програмного забезпечення, зростання чисельності користувачів тощо [64].

За змістом ризики кібербезпеки прийнято класифікувати наступним чином:

— ризики щодо конфіденційності інформації;
— ризики щодо цілісності інформації;
— ризики щодо доступності інформації [54].

Під конфіденційністю інформації розуміють установлений режим її розповсюдження. Цей режим включає:

— коло осіб, наділених доступом до даних (повністю або частково);
— обсяг повноважень окремих осіб щодо даних (ознайомлення, зміна, розповсюдження тощо);
— нормативні засади захисту інформації;
— процедуру поширення інформації (випадки, обсяг, порядок тощо) [47].

Конфіденційність та цілісність даних є тісно пов'язаними ознаками, які полягають у відсутності несанкціонованих змін обсягу, змісту, структури послідовності, та форми викладу інформації, як в цілому, так і щодо її окремих частин. Доступність даних – це характеристика, яка передбачає об'єктивну

можливість санкціонованого доступу компетентних осіб до інформації та її цільового використання [32].

Реалізація ризиків кібербезпеки підприємства обумовлює значні матеріальні втрати. Це може бути як заподіяння підприємству майнової шкоди у формі реальних збитків і втраченої вигоди, так і заподіяння моральної шкоди, зокрема, щодо ділової репутації. Збитки, завдані реалізацією ризиків безпеки інформаційної системи підприємства, можуть виражатися у формі пошкодження устаткування, програмного забезпечення, втрати даних тощо [15].

Завдана шкода полягає у тимчасовому повному або частковому блокуванні діяльності підприємства, внаслідок чого унеможливлюється укладення чи належне виконання вигідних договорів. Цьому слідує, як мінімум, втрата доходу, який міг би бути отриманим за звичайних обставин, а як максимум, претензійно-позовні формальності, ініційовані незадоволеними кредиторами [55].

Окрім того, у випадку реалізації кіберзагроз підприємство може бути притягнуто до юридичної відповідальності, передусім, цивільної та господарської, за порушення нормативно-правових та договірних засад захисту інформації. Це стосується і персональних даних, якими володіє або розпоряджається суб’єкт господарювання, наприклад, персональних дані працівників, клієнтів тощо, і таємної, конфіденційної інформації, наприклад, щодо господарської діяльності договірних контрагентів (інших підприємств) [11].

2.3 Управління ризиками у процесі обробки інформації

Говорячи про запобігання реалізації ризиків кібербезпеки підприємства, не можна оминути увагою поняття управління ризиками у процесі обробки інформації. В цілому, під управлінням ризиками у менеджменті розуміють комплекс (систему) заходів, спрямованих на забезпечення мінімально можливих показників ризиків, які супроводжують функціонування бізнесу [62].

Ефективне управління ризиками кібербезпеки має важливе значення для безпеки підприємства загалом. Ризик-менеджмент є триваючою діяльністю, яка включає такі етапи:

— дослідження;
— визначення стратегії;
— вплив;
— контроль [51].

За загальним правилом, управління ризиками розпочинається із аналізу, який передбачає з'ясування сфери, типу, характеру існуючих загроз, оцінки їх ступеня та можливих наслідків впливу на діяльність підприємства у випадку реалізації. Саме це і становить зміст дослідження ризиків. У контексті кібербезпеки підприємства дослідження ризиків, по суті, зводиться до вивчення уразливості інформаційної системи. Цю ознаку (показник) детальніше вже було розглянуто вище [52].

Еволюція методики управління ризиками кібербезпеки підприємства включає послідовність таких підходів:

— технічний;
— менеджерський;
— інституційний [34].

Технічний підхід зосереджений передусім на захисті окремих елементів інформаційної системи:

— Апаратного устаткування;
— програмного забезпечення;
— Даних;

Технічні методи зводяться, в цілому, до підготовки сценаріїв на випадок збою системи та резервного копіювання даних. Під резервним копіюванням розуміють процес створення копії даних з носія, призначений для відновлення цих даних у разі їхнього пошкодження (зміни) чи втрати (видалення) [29].

Менеджерський підхід до управління ризиками кібербезпеки полягає у включенні безпеки інформаційної системи до комплексної політики безпеки

підприємства. Такий підхід не виключає застосування технічних методів, проте значно ширшим, здатним забезпечувати не лише збереження інформації, але і її належну конфіденційність [28].

Інституційний підхід, що використовується для управління ризиками безпеки інформаційної системи, який включає такі елементи:

— стандартизацію безпеки інформаційної системи;
— атестацію рішень щодо кібербезпеки;
— уніфікацію механізмів для вимірювання безпеки інформаційної системи на підприємстві.

Стандартизація передбачає запровадження у практику господарської діяльності високих вимог (стандартів) щодо безпеки інформаційної системи, а також механізмів забезпечення дотримання цих вимог. Атестація передбачає незалежну оцінку рішень щодо кібербезпеки, зокрема, їхнього коефіцієнта корисної дії (необхідності та ефективності відносно витрат). Уніфікація механізмів для вимірювання безпеки ІС забезпечує можливість ефективного моніторингу [19].

Висновки до розділу

Прийшли до висновку, що аналіз ризиків є вихідними даними для визначення стратегії ризик-менеджменту. Під стратегією розуміється цілісне (системне) і перспективне (відносно тривале у часі) бачення мети, завдань, напрямків управління ризиками, а також вибір відповідних методів, засобів та планування необхідних ресурсів (матеріальних, кадрових тощо).

Вплив на ризики, по суті, є основою ризик-менеджменту. Вплив здійснюється щодо ризиків, виявлених у процесі дослідження бізнес-середовища (наприклад, інформаційного середовища підприємства на предмет уразливості). Здійснення впливу на ризики зазвичай відбувається у межах окресленої стратегії. Варто розуміти, що стратегія є орієнтиром, а не докладним планом конкретних дій, а відтак, розробка стратегії управління ризиками не замінює прийняття рішень при безпосередньому впливі на ризики.

Метою впливу є приведення показників існуючих ризиків до їхніх мінімально можливих значень, відповідно до умов. Після досягнення зазначеної мети, а також за умови стартових задовільних показників, виявлених ще на етапі дослідження, необхідно на постійній основі здійснювати контроль за змінами.

3. МЕТОДИ АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Загальна характеристика методології аналізу ризиків інформаційної безпеки

В даний час застосовується кілька десятків методів оцінки та оцінки ризику інформаційної безпеки. Загалом їх можна розділити на 3 групи:

— кількісні методи;
— якісні методи;
— змішані методи[43].

Якісна оцінка ризику – це найчастіше суб'єктивна оцінка, заснована на передовій практиці та досвіді. Результатом такої оцінки є списки загроз разом із відносними рейтингами ризику (низький, середній, високий). Ці методи дуже гнучкі і відкриті для всіх типів модифікацій. Як результат, вони дають можливість організації забезпечити швидкі та економічно ефективні результати у сфері визначення небезпеки та безпеки. Однак, завдяки цій гнучкості, обсяг та вартість оцінки можуть сильно відрізнятися. Тому, залежно від наявного бюджету, ступінь оцінки ризику може змінюватися з часом[27].

У якісному аналізі всі ризики та потенційні наслідки ризику представлені описово. Він передбачає використання сценаріїв подій та визначення ефектів від потенційного ризику. Вони можуть містити багато деталей, які допоможуть вжити конкретних дій та вибрати правильні гарантії. Зазвичай використовуються різні масштаби, описані для конкретних ситуацій та будь-яких винятків[20].

Переваги використання якісних методів:

— розрахунки прості та зрозумілі;
— не потрібно кількісно оцінювати наслідки та частоту загроз;
— визначення загальних ознак значущих сфер ризику, які потребують уваги;
— здатність враховувати при оцінці таких аспектів, як, наприклад, імідж компанії, організаційна культура, репутація тощо;
— можливість використання за відсутності конкретної кількісної інформації та даних або ресурсів, яка може знадобитися для кількісних методів[17].

У кількісному підході при оцінці ризику найважливішим є визначення двох основних параметрів, тобто значення ефекту та ймовірності виникнення даного ризику. Ефекти можна визначити шляхом оцінки результатів подій або шляхом екстраполяції на основі даних минулого. Наслідки можуть виражатися в різних категоріях (грошові, технічні, операційні)[13].

Якість усього аналізу залежить від точності вказаних значень та статистичної валідації використовуваної моделі. До переваг кількісного методу можна віднести можливість кількісно встановити на основі статистичних даних розмір потенційних збитків та ймовірність їх виникнення, в результаті реалізації загроз, а також рівень існуючих ризиків[17].

Оптимальним може бути змішаний метод. Як кількісні, так і якісні методи мають свої слабкі сторони. З одного боку, якісний метод є надто загальним, не точно визначає будь-які потреби в інформаційній безпеці, з іншого боку кількісний, не дає інформації про аналіз витрат з точки зору впровадження нових стандартів. З цієї причини більшість компаній використовують поєднання цих двох підходів. Якісний аналіз, заснований на сценарних методах, використовується для виявлення всіх областей ризику та впливу, при цьому використовуючи кількісний аналіз для визначення витрат наслідків ризику. Це, звичайно, призводить до значного збільшення знань про процеси, що здійснюються в організації, та покращують усвідомлення компаніями потенційних ризиків[13].

3.2. Методи та стандарти аналізу інформаційної системи

Модель згідно стандарту ISO / IEC 27001: 2005. Модель процесу оцінки ризику інформаційної безпеки, є підходом до питання, що обговорюється, поширюється та описується стандартом ISO / IEC 27001: 2005. Він описує елементи, які слід знайти при побудові методології оцінки ризиків. Цей підхід є вигідним, оскільки стандарт безпеки не передбачає використання однієї конкретної організації методології, тим самим надаючи свободу вибору. Це виправдано насамперед різним рівнем зайнятості в організації, специфікою бізнесу, сферою діяльності, структурою зайнятості тощо.

Однак стандарт вимагає зазначення конкретного методу оцінки ризику. Це перш за все для того, щоб методичний підхід до оцінки ризику дозволив, з одного боку, порівнювати результати за часом, а також повторюваність результатів. Необхідно додатково розробити критерії прийняття ризику та вказати прийнятні рівні ризику. В даний час існують різні методи оцінки ризику, які були опубліковані та широко використовуються організаціями. Звичайно, організаціям можна використовувати власні методи, розроблені на основі власного досвіду[4].

Стандарт ISO / IEC 27001 не вказує, який саме метод найкраще використовувати, хоча він ілюструє методи оцінки ризиків, обговорені в ISO / IEC TR 13335-3, Інформаційні технології - керівні принципи управління інформаційною безпекою.

Стандарт ISO / IEC 13335-3142, випущений у 1998 році, є частиною п'ятипозиційного стандарту, присвяченого інформаційним технологіям, і є набором настанов (вказівок) для осіб, що займаються управлінням безпекою інформаційних систем. Містить способи формування трирівневої політики безпеки, розробляє питання аналізу ризиків, виконання плану безпеки та реагування на інциденти, а також представлені методики оцінки ризику інформаційної безпеки[2].

Матриця із заданими значеннями це метод що включає ідентифікацію основних активів в організації. Потім оцінює кожен актив на бальній основі (використовуючи значення від 0 до 5) та визначає вразливості та загрози (використовуючи якісні терміни S - низький, M - середній, H - високий). На основі цих трьох параметрів (значення активів, рівень вразливості та загрози)визначається ризик за допомогою матриці із заздалегідь заданими значеннями[8]. Приклад практичного застосування матриці із заданими значеннями проілюстровано на рисунку 3.1.

	Рівень загроз	Низькі			Середні			Високі		
	Рівень вразливості	S	M	H	S	M	H	S	M	H
Значення активу	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

Рис. 3.1. Матриця із заданими значеннями

Значення активів, а також рівень загрози та вразливості правильно поєднуються в матриці. Конкретні ризики для кожної комбінації цих трьох параметрів встановлюються, приймаючи точкові значення за шкалою від 1 до 9.

Для кожного аналізованого активу слід враховувати всі загрози та вразливості. Іноді існують однакові вразливості без відповідної загрози. У такому випадку слід вважати, що рівень загрози для даного активу низький. Наприклад, якщо значення активу становить 3, загроза висока, а рівень вразливості низький, ризик - 5. Якщо значення активу становить 2, наприклад, рівень загроз низький, а рівень вразливості високий, ризик - 4.

Оцінка ризиків за процедурою дозволяє порівняти різні загрози з різними ефектами та ймовірністю виникнення. Результатом використання вищевказаної процедури є список, який класифікує загрози за рейтингом від найбільшої до

найменш значної загрози для організації. У деяких випадках може знадобитися включення грошової оцінки активів в емпіричному масштабі[3].

Метод Cortney. перше офіційне визнання питання оцінки ризиків, пов'язаних із безпекою IT-систем, було представлено у червні 1974 р. У публікації FIPS 31 у праці під назвою «Фізична безпека та автоматизована обробка даних Фізична безпека та управління ризиками». Метод аналізу ризиків, заснований на роботі Роберта Кортні, описаному в FIPS 31 (Публікація Федеральних стандартів обробки інформації), представлений в публікації FIPS 65 "Настанови щодо аналізу ризику автоматичної обробки даних" (Керівництво щодо ризику автоматичної обробки даних) Аналіз) 1979 р. - один із перших, а також найбільш широко використовуваний і цитується в літературі.

У цьому методі ризик втрати безпеки інформаційних систем розглядається в контексті трьох основних ознак: конфіденційність, доступність та цілісність. Він виражається у сумі можливих втрат, спричинених виникненням заданої загрози[2].

Метод оцінки ризику, запропонований Робертом Кортні, є найбільш відомим і вважається основою для оцінки ризику, пов'язаного із безпекою інформаційних систем до сьогодні.

Кортні визначає два основні компоненти ризику (R):

P — ймовірність того, що дана загроза виникне певну кількість разів протягом заданого часу.

C — величина потенційних втрат, що виникають внаслідок виникнення загрози.

Значення ризику, пов'язаного з безпекою інформаційних систем, є декартовим добутком, вираженим формулою:

(3.1)

У цій же роботі також був запроваджений перший формальний метод оцінки ризику, пов'язаного із безпекою інформаційних систем, що містить простий описовий алгоритм кількісної оцінки ризику, який називається ALE (річна тривалість втрат).

Алгоритм обчислення значення передбачуваних річних втрат, ALE — величина, визначена за формулою 3.2.

$$ALE = SLE \cdot ARO \quad \textbf{(3.2)}$$

Де *ARO*— Щорічна частота виникнення - це орієнтовна частота події, що спричинила втрату,

SLE— Очікувана тривалість разової втрати - це сума очікуваної втрати, що виникає внаслідок одного випадку події, що спричинила дану втрату, виражена в грошах - ця сума визначається за формулою 3.3.

$$SLE = AV \times EF \quad \textbf{(3.3)}$$

Де *AV*— цінність активів, тобто грошова вартість ресурсу, до якого відноситься аналізована подія, що спричинює дану втрату,

EF— Коефіцієнт експозиції визначає відсоток вартості активів AV, який втрачається в результаті однієї події, що спричинить задану втрату.

Для спрощення процесу обчислення розміру ALE на основі формул 3.2. та 3.3. використовується формула 3.4

(3.4)

Де *f*— індекс, що визначає передбачувану частоту події, що викликає задану втрату, значення якої з набору вказані в документі FIPS 65,

i— індекс, що визначає передбачувану суму збитків, спричинених виникненням події, що спричинила цю втрату, значення якої з множини згадується в FIPS 65.

Універсальність оцінки ризику інформаційних систем за методом Кортні випливає з простоти використовуваного підходу, та інтуїтивності обчислення ALE, а також від того, що це був один з перших формалізованих методів аналізу проблеми оцінки ризиків, пов'язаних із безпекою інформаційних систем, який був прийнятий як стандарт уряду США[9].

Метод Фішера, метод, запропонований Робертом Фішером , є розробкою методу Кортні.

Метод Фішера - це комплексний метод розробки рішень безпеки інформаційних систем. У цьому методі процес управління ризиками інформаційної системи складається з п'яти фаз:

— Інвентаризація ресурсів

— Ідентифікація небезпек. Визначені загрози поділяються на одинадцять груп загроз, які є розширенням шести груп загроз, виявлених методом Кортні.

— Оцінка ризику. Рівень ризику для інформаційної системи розраховується на основі інформації, зібраної на першій фазі, за допомогою апарату Кортні, Метод Кортні (описаний у FIPS 65 як ALE).

— Проектування механізмів управління. На цій фазі розробляються механізми управління у сфері запобігання, виявлення та вдосконалення рівня безпеки інформаційної системи. Для конкретного класу ризику вибирається відповідний клас захисту. Принциповим для цієї фази є підбір гарантій, відповідних потребам - рівню ризику та вартості ресурсів.

— Аналіз витрат. Виявлені механізми зменшення ризику підлягають аналізу з точки зору їх економічної прибутковості, коли максимальна вартість безпеки даної IT-системи не може бути вище загальної вартості цієї системи[5].

Основна мета оцінки ризику за методом Фішера - розробка політики безпеки та планів захисту окремих інформаційних систем. Новизною цього методу стала розробка економічно ефективних механізмів зменшення ризику, пов'язаного з інформаційними системами.

Метод Паркера, Метод управління ризиками, пов'язаний із безпекою інформаційних систем, розроблений Девідом Паркером у 1981 році на замовлення Інституту комп'ютерної безпеки складається з п'яти фаз:

— Ідентифікація та оцінка ресурсів.

— Ідентифікація загроз. За допомогою цього методу він здійснюється відповідно до належності кожної загрози до конкретних категорій, запропонованих Паркер, наприклад джерела загроз, мотивів сторін загрози або суми збитків, завданих ними.

— Оцінка ризику. Це відбувається за допомогою методу Кортна, розширеного Матрицею аналізу експозиції. При побудові цієї матриці передбачалося, що значимість загроз є функцією кількості людей, які можуть спричинити втрату.

Це припущення призводить до аналізу ризику за окремими професійними групами.

— Ідентифікація, вибір та реалізація безпеки.

— Рекомендації щодо програми безпеки.

Основна мета оцінки ризику за допомогою методу Паркера - розробка політики безпеки та планів захисту окремих інформаційних систем. Елементи методуКортні також використовуються в цьому методі розширено, щоб включити якісну оцінку ризику та зменшити вплив людського фактору на ризики. У ньому також важливий процес управління безпекою інформаційних систем, що відрізняє його від інших методів[9].

Британський метод CRAMM (CCTA Risk Analysis Management Methodology), розроблений CCTA (Урядове центральне комп'ютерне та телекомунікаційне агентство), збагачений спеціальним програмним забезпеченням, був прийнятий як державний стандарт оцінки ризиків та управління безпекою інформаційної системи. Це метод, при якому весь процес управління ризиками в інформаційній системі складається з трьох послідовних етапів:

— Ідентифікація та оцінка ресурсів, в яких визначається детальний обсяг аналізу інформаційних систем щодо апаратного, програмного забезпечення та даних. Індивідуальне оцінювання проводиться для всіх виявлених та описаних фізичних ресурсів. Що стосується програмного забезпечення та даних, то оцінка проводиться на основі передбачуваної втрати внаслідок недоступності, знищення, розкриття чи несанкціонованих змін. Для всіх описаних ресурсів проводиться оцінка значущості даного ресурсу для організації та впливу порушень у функціонуванні даного ресурсу на функціонування всієї організації (за шкалою від 1 до 10).

— Оцінки загрози та вразливості для виділених ресурсів. Цей етап починається з групування (частково автоматичного) ідентифікованих та описаних ресурсів на три можливі типи: інформація, програмне забезпечення та середовище. Потім встановлюються відносини між окремими групами, і лише тоді можна оцінити

рівень загроз та вразливості. Списки загроз автоматично формуються для окремих груп ресурсів і визначається оцінка рівня загрози для кожної з цих груп за п'ятибальною шкалою, від дуже низької до низької, середньої, від високої до дуже високої. Для оцінки вразливості була прийнята трирівнева шкала: низька, середня та висока. Виходячи зі значення ресурсів, рівня загрози та вразливості, значення ризику визначається за семибальною шкалою, де 1 означає найменший необхідний захист, а 7 означає дуже високі вимоги.

— Управління ризиками, яке полягає у виборі рекомендованих механізмів контролю та захисту з існуючої бази даних. Ця база даних містить понад 3 000 елементарних вимог безпеки, погоджених із службами безпеки та відповідними організаціями зі стандартизації. Реалізація цих гарантій значно зменшує попередньо виявлені загрози[10].

Метод TRA для оцінки загрози та ризику розроблений для федеральних відомств і є офіційним набором керівних принципів у галузі управління ризиками, пов'язаними із безпекою інформаційних систем уряду Канади. Завдяки високій якості дослідження та можливості його використання в установах, які не мають урядового профілю, він широко розповсюджується та адаптується до місцевих потреб. Цей метод сильно інтегрований із життєвим циклом розвитку системи (SDLC), аналогічним життєвому циклу безпеки інформаційної системи. Крім того, він розширений елементами звітності про ризики.

У методі TRA, як і в попередніх методах, є чітко визначені фази:

— Планування дій.

— Підготовка, під час якої оцінюється дійсність атрибутів безпеки для даної інформаційної системи (конфіденційність, доступність, цілісність).

— Аналіз - ключова фаза цього методу, включаючи аналіз небезпеки та оцінку ризику.

— Рекомендації. Метод TRA передбачає чотири основні класи управління ризиками, якими автоматично керується на наступному етапі.

— Рішення зменшити, прийняти, перенести чи уникнути ризику.

— Вказання вимог безпеки.
— Вибір заходів безпеки, відповідних потребам (адміністративних, технічних, фізичних та особистих);
— Побудова та впровадження заходів безпеки, що знижують ризик до прийнятного та перевіреного рівня.
— Сертифікація за допомогою тестів.
— Рішення про акредитацію.
— Акредитація.
— Технічне обслуговування та експлуатація.
— Можливі рішення про зміни

Елементом, який відрізняє цей метод від інших, є введення до аналізу таких елементів, як значення вразливості, ймовірність загроз, наслідки загроз, ефективність безпеки тощо[5].

Тобто оцінка прогалин та критичних ресурсів для дій, - це керівні принципи, створені в 2001 році в університеті Карнегі-Меллона. Методика використовується, серед інших з боку армії США та все більшою кількістю більших організацій[4].

Метод OCTAVE визначає ризики на основі стратегічної оцінки та планування методів безпеки. Він адресований всім типам організацій. Методологія базується на припущенні, що працівники організації несуть відповідальність за створення стратегії організаційної безпеки. Реалізація своїх припущень повинна здійснюватися через невелику міждисциплінарну команду людей (від трьох до п’яти співробітників організації), які збиратимуть та аналізуватимуть інформацію, визначають стратегію застосування планів безпеки та дій на основі ризиків організаційної безпеки. Для ефективного впровадження методології OCTAVE команда повинна мати широкі знання про ділову діяльність організації та процеси безпеки [8].

Методологія базується на трьох етапах.

— Перший етап складається з всебічного аналізу організаційних ресурсів, виявлення існуючої практики, огляду вимог безпеки, діагностики організаційних прогалин та існуючих загроз.
— Другий етап спрямований на виявлення технологічних прогалин.
— Третій етап базується на розробці стратегії захисту та плану управління ризиками.

3.3 Реалізація системи управління ризиками безпеки некомерційного комунального підприємства на основі стандарту ISO/IEC TR 13335

В 2016 році команда міністерства охорони здоров'я на чолі з Уляною Супрун розпочали комплексну медичну реформу. Одними із складових було перетворення лікарень, амбулаторій і поліклінік із бюджетних закладів так званих ЗОЗ(заклади охорони здоров'я) в некомерційні комунальні підприємства. Також реформа передбачає оцифрування реформованих медичних закладів створення електронної медичної книжки, електронної реєстратури, електронної історії хвороби, електронної черги, електронний кабінет лікаря і електронний кабінет пацієнта, випуск електронних рецептів і направлень тощо[71]. Актуальність проблематики неможливо переоцінити оскільки проблема нелегального обігу наркотичних речовин за фальшивими медичними рецептами набула масового характеру.Саме тому було вирішено створити модель системи управління ризиками для некомерційного комунального підприємства.

Розуміючи фінансову ситуацію медичних установ які функціонують лише за рахунок субвенцій з державного бюджету та дотацій місцевої влади, та зважаючи ринкові вимоги та запити пацієнтів варто розглянути можливість впровадження системи управління ризиками інформаційної безпеки на основі стандарту ISO / IEC TR 13335 у новостворених некомерційних комунальних підприємств. Зважаючи на характер діяльності, було потрібно детальне планування окремих етапів роботи, пов'язаних із проектуванням, розробкою та впровадженням системи. Робота над цим проектом сприяла створенню нових системних рішень, а також створенню спеціальної методології для боротьби з

усіма інцидентами безпеки, людського фактору або порушеннями політики безпеки [6].

Прикладів інформації в закладі охорони здоров'я є безліч: бухгалтерські документи, персональна інформація пацієнтів та працівників, фінансова інформація, конфіденційна інформація, база електронних рецептів, інформація про ресурси (технології, патенти, програмне забезпечення), бази даних, системна документація, посадові інструкції, результати аудиту, звіти, плани коригуючих та профілактичних заходів, листування з постачальниками, замовниками, договори, інформація про системну та фізичну безпеку, а також інформація що належить третім особам тощо [71].

Оцінка інформації спрямована на перегляд усієї інформації, яка присутня в даній установі, та визначення її класифікація.

Це дасть можливість здійснити відповідні процеси, процедури та інструкції для захисту інформації, пропорційно до її важливості для установи. Суть полягає у забезпеченні належного захисту з точки зору негативних наслідків, спричинених втратою або небажаною модифікацією цієї інформації. Інформація закладу охорони здоров'я є об'єктом особливої важливості і, що очевидно є об'єктом цікавості зловмисників. наприклад персональні дані пацієнтів можуть бути передані третім особам для формування так званих клієнтських баз та подальшого їх продажу.

Як за основу для реалізації системи управління ризиками візьмем метод Міри ризику. Міра ризику метод який представлений у стандарті ISO / IEC TR 13335.Вихідним пунктом є виявлення всіх загроз. Потім оцінюються два параметри за шкалою від 1 до 10 - вартість активу (вартість виникнення інциденту інформаційної безпеки) та ймовірність виникнення загрози. Значенням ризику є добутком цих двох параметрів [1]. Метод проілюстровано в таблиці 3.1.

Таблиця 3.1

	Назва загрози	**Визначення виявлених ризиків**	**збитки (пов'язані з виникненням інциденту для компанії (1-10 низький, високий)**	**Ймовірність виникнення загрози (1-10)**	**Міра ризику**
1	Крадіжка даних	Неправомірне використання інформації що належить підприємству або третім особам, і зберігається на її носіях.	8	10	80
2	Використання інформації, наданої в пропозиції замовником	Використання клієнтом або потенційним клієнтом інформації наданою підприємством без відома та згоди	10	9	90
3	Крадіжка обладнання	Неправомірне вилучення обладнання що належить підприємству.	10	8	80
4	Несанкціонований доступ до мережі	Проникнення до мережі без права доступу	10	8	80
5	Злом системи	Несанкціоноване заволодіння доступу доінформаційної системи а також до інформації що в ній зберігається	10	8	80
6	Навмисна несанкціонована модифікація даних	Умисні дії особи, яка не має прав на модифікацію. інформації	10	7	70
7	Некомпетентність зі сторони персоналу	Невиконання персоналом політики безпеки через недостатню кількість знань	9	9	81
8	Вірусна атака	Ураження вірусом систем, дисків або окремих файлів	6	7	42
9	Порушення конфіденційності	Доступ до конфіденційної інформації несанкціонованими особами	6	6	36
10	Соціальна інженерія	Використовування методів соціальної інженерії для реалізації правопорушення	6	5	30
11	Пожежа	Пошкодження майна в результаті пожежі	10	3	30
12	Стихійні лиха	Пошкодження систем та обладнання підприємства в результаті стихійного лиха	10	2	20
13	Антропогенні катастрофи	Аварії та катаклізми спричинені діяльністю людини	10	2	20

Розроблена таблиця з загрозами та збитками понесеними у випадку інциденту, та ймовірність виникнення події сприяє прозорому представленню та оцінці окремих ризиків. Методом вимірювання окремих ризиків ймовірність ризику та можливі збитки що виникають внаслідок його реалізації. Рейтинг ймовірності та збитки виражаються у вигляді шкали балів від 1 до 10, де 1 означає низьку ймовірність ризику або збитку, а 10 дуже високу. Добуток цих двох значень коливається навколо значення в межах від 1до 100. Чим більша кількість балів, тим вищий ризик. Формула для оцінки ризику загрози в даному випадку набуває вигляду: оцінка ризику для даної загрози рівняється до оцінки ймовірності ризику помноженого збитки від виникнення загрози.

Після отримання результатів ми можемо класифікувати ризики згідно отриманих балів вразливості, які встановлюються рівні:

— до 30 - низький ризик,
— до 50 - середній ризик,
— вище 60 - високий ризик.

3.4 Висновки до розділу

У даному розділі нами опрацьовано загальні методи і способи аналізу ризиків інформаційних систем, зокрема розглянули якісні, кількісні і змішані методи оцінки ризику, порівняв їх переваги та недоліки а також доцільність використання. Описано стандарти і методи оцінки ризиків, реалізовано на основі міжнародного стандарту ISO/IEC TR 13335 систему управління ризиками безпеки некомерційного комунального підприємства – закладу охорони здоров’я.

4 РОЗРОБКА МОДЕЛІ ПОРУШНИКА

4.1 Теоритичні відомості

Порушник - це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо. Відносно АС порушники можуть бути внутрішніми (з числа персоналу або користувачів системи) або зовнішніми (сторонніми особами).

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо.

По відношенню до автоматизованої системи порушники можуть бути внутрішніми або зовнішніми.

4.2 Реалізація моделі порушника

Метою порушника можуть бути отримання необхідної інформації у потрібному обсязі та асортименті (Ц1), мати можливість вносити зміни в інформаційні потоки (Ц2) та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей (Ц3).

За рівнем можливостей, що надаються їм засобами автоматизованої системи, порушники поділяються на тих, хто має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації (Р1), тих, хто має можливість створення і запуску власних програм (Р2) та тих, хто має можливість управління функціонуванням автоматизованої системи, впливу на базове програмне забезпечення системи і на склад і конфігурацію її устаткування (Р3).

За рівнем знань про автоматизовані системи усіх порушників можна класифікувати як таких, що мають невисокий рівень знань інформаційних

технологій, володіють інформацією про функціональні особливості автоматизованої системи (Зн1), тих, що володіють середнім рівнем знань інформаційних технологій, мають досвід роботи з технічними засобами автоматизованої системи та їхнього обслуговування (Зн2), тих, що володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації автоматизованої системи (Зн3) та тих, що володіють інформацією про функції та механізм дії засобів захисту (Зн4).

За використовуваними методами і способами порушників можна класифікувати на тих, хто використовує виключно агентурні методи одержання відомостей (Сп1), тих, хто використовує пасивні технічні засоби перехоплення інформаційних сигналів (Сп2), тих, хто використовує виключно штатні засоби автоматизованої системи або недоліки проектування системи захисту інформації для реалізації спроб НСД (Сп3) та тих, хто використовує засоби активного впливу на автоматизовану систему, що змінюють її конфігурацію (Сп4).

За місцем здійснення дії можуть класифікуватись на тих, хто не має доступ на контрольовану територію (М1), тих, хто має доступ до КТ, але не має доступу до технічних засобів АС (М2), на тих, хто має доступ до робочих місць кінцевих користувачів системи (М3), та тих, хто має доступ до засобів адміністрування системи (М4).

Порушники можуть діяти в робочий (Ч1) та в неробочий час (Ч2). Для некомерційного комунального підприємства порушників можна розділити на наступні групи (дирекція підприємства, як розпорядник підприємства та за відсутності мети порушення у моделі не враховується):

Внутрішні порушники(робочий персонал) :

— ПВ1 - системний адміністратор.
— ПВ2 – програмісти, тестувальники.
— ПВ3 – керівники відділів.
— ПВ4 – бухгалтер, секретар, юрист.
— ПВ5 – фахівці з забезпечення зв’язку.
— ПВ6 – прибиральник, охоронець.

Порушники зовнішні:

— ПЗ1 – партнери та клієнти.

— ПЗ2 – технічний персонал з обслуговування будівлі та комунікацій.

— ПЗ3 – кримінальні структури.

— ПЗ4 – хакери.

Використовуючи наведені класифікації, була побудована модель порушника, наведена у рисунку 4.1. Рівні небезпеки порушника для підприємства визначені як вірогідність реалізації загрози цим порушником.

Порушник	Рівень знань ІТ	Рівень знань про ОІД	Місце дії	Час дії	Рівень можли-востей	Методи і способи	Мета	Рівень небезпеки
ПВ1	Зн3	Зн4	М4	Ч1,Ч2	Р3	Сп3, Сп4	Ц1, Ц3	високий
ПВ2	Зн3	Зн3	М3	Ч1	Р2	Сп3	Ц1, Ц3	середній
ПВ3	Зн2	Зн3	М3	Ч1	Р1	Сп3	Ц1, Ц3	середній
ПВ4	Зн1	Зн2	М3	Ч1	Р1	Сп3	Ц1, Ц3	низький
ПВ5	Зн2	Зн4	М3	Ч1	Р1	Сп3	Ц1	середній
ПВ6	Зн1	Зн2	М3	Ч1	-	Сп2	Ц1, Ц3	низький
ПЗ1	Зн3	Зн1	М2	Ч1	-	Сп3	Ц1	низький
ПЗ2	Зн1	-	М1	Ч1,Ч2	-	Сп1	Ц1-Ц3	середній
ПЗ3	Зн4	-	М1	Ч2	-	Сп3	Ц3	низький
ПЗ4	Зн3	-	М1	Ч2	-	Сп4	Ц1-Ц3	низький

Рис. 4.1 Модель порушника на прикладі некомерційного комунального підприємства

4.3 Висновки до розділу

Розглянуто теоретичні відомості про правопорушників і модель порушника, а також розроблено модель порушника на прикладі некомерційного комунального підприємства. Для мінімізації ризику втрати та компрометації цінних інформаційних ресурсів підприємства через реалізацію кіберзагроз може бути запропоновано зниження ризику за допомогою допоміжних систем або найму спеціалістів з інформаційної безпеки та попередження ризику за допомогою попереднього аналізу ризику втрати інформації, яка підлягає захисту.

5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

5.1 Мета та завдання

Завданням та метою цього розділу є розрахунок економічної ефективності застосування методу оцінки ризику та запровадження мір щодо уникнення ризику кіберзагроз. Для визначення ефективності необхідно розрахувати:

— експлуатаційні витрати для зниження ризику за допомогою засобів захисту;
— витрати на кібербезпеку при застосуванні методу оцінки ризиків;
— можливі витрати на запровадження необхідних мір та зменшення ризику з можливими втратами;

Система вимог щодо зменшення ризику повинна бути настільки сповнена, щоб її виконання дозволяло повністю охоплювати усі можливі істотні ризики та загрози. Тільки в цьому випадку можна буде виміряти рівень довіри до безпеки використовуваної системи рівнем виконання вимог. До проблем безпеки автоматизованої інформаційної системи прийнято використовувати термін - «інформаційна безпека». При виконанні системи вимог інформаційної безпеки можуть виникнути наступні проблеми:

— виконання всіх можливих вимог щодо забезпечення ІБ може бути неможливо через занадто високу вартість їх реалізації;
— вимоги щодо безпеки можуть не виконуватися через відсутність досить ефективного контролю за виконанням вимог;
— вимоги можуть не виконуватися, оскільки вони погано засвоєні виконавцями.

У всіх трьох випадках контроль за виконанням вимог може дати великий позитивний ефект. Якщо частина вимог не може бути реалізована через нестачу коштів на їх реалізацію, контроль повинен дозволити не випускати з виду існуючі проблеми і вирішувати їх у міру появи коштів на підвищення інформаційної безпеки з урахуванням показників важливості вирішення зазначених проблем. При відсутності ефективного контролю за виконанням вимог з боку виконавців можуть проявлятися тенденції оптимізувати свою роботу за рахунок ігнорування деяких вимог з безпеки. Тому постійний контроль

за виконанням вимог крім іншого покликаний переконати виконавців важливістю виконання вимог.

В системах, де організований контроль всіх вимог, як правило, крім великого числа інструкцій, наказів, законодавчих та підзаконних актів, в яких формуються вимоги, складаються списки вимог по підконтрольним структурам і процесам. Наявність такого роду списків дозволяє як контролерам, так і виконавцям швидше зрозуміти вимоги, швидше освоювати систему вимог і, відповідно, краще їх виконувати.

5.2 Розрахунок витрат на впровадження системи управління ризиками інформаційної безпеки підприємства

Обстеження підприємства:

B0 = 5000 грн.;

Проектування системи захисту:

B1= 5000 грн.;

Налаштування системи захисту:

B2 = 3000 грн.;

Розробку правил кореляції для сценаріїв виявлення інцедентів:

B3 = 4000 грн.;

Розробку регламенту реагування на інциденти кібербезпеки:

B4 = 3000 грн.;

Розробку інструкцій оператора/аналітика/користувача:

B5 = 2000 грн.;

Вартість реалізації проекту рівна сумі наданих послуг і відповідно, розраховується за формулою:

$$B= B0+B1+B2+B3+B4 + B5 = 5000+5000+3000+4000+3000+2000=22000$$

Орієнтовна вартість реалізації проекту системи аналізу ризиків інформаційної безпеки: 22000 грн.

5.2 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Розробку поділяють на декілька етапів, що дозволить полегшити і структурувати виконання розробки методики.

Основні етапи при виконанні розробки методики наступні:

1. Обґрунтування необхідності використання методики безпечного зберігання інформації.
2. Обстеження середовища в якому запропонована методика.
3. Визначення потенційних загроз інформації.
4. Розробка документів політики безпеки.
5. Складання плану захисту.
6. Підготовка до введення в дію методики.
7. Попереднє випробування методики.
8. Введення в дію методики.

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу або попередній досвід. До таких відносять і тривалість встановлення програмного забезпечення та програм шифрування. Виконавцем усіх операцій по розробці методики безпечного зберігання інформації на носіях є позаштатні працівники служби захисту інформації. Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та час їх виконання

п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Обґрунтування необхідності використання методики безпечного зберігання інформації	Інженер	8
2	Обстеження середовища в якому запропонована методика.	Інженер	16
3	Визначення потенційних загроз інформації.	Інженер	8
4	Розробка документів політики безпеки.	Інженер	16
5	Складання плану захисту.	Інженер	12
6	Підготовка до введення в дію методики.	Інженер	24
7	Попереднє випробування методики.	Інженер	24
8	Введення в дію методики.	Інженер	36
Разом			144

6.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S\,, \qquad (6.7)$$

де W – необхідна потужність, кВт; T – кількість годин роботи обладнання; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів (1,40 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 1,68 грн.

Потужність комп'ютера для створення проекту – 400 Вт, кількість годин роботи обладнання згідно таблиці 3.1 –144 години.

Тоді,

$$З_в = 0{,}4 \cdot 144\ 1{,}68 = 96{,}76 \text{ грн.}$$

5.3 Висновки до розділу

В даному розділі розраховано експлуатаційні витрати для зниження ризику за допомогою засобів захисту, витрати на кібербезпеку при застосуванні методу оцінки ризиків, можливі витрати на запровадження необхідних мір та зменшення ризику з можливими втратами а також розраховано загальну вартість проекту системи аналізу ризиків інформаційної безпеки підприємства, на прикладі некомерційного комунального підприємства. Виправданість реалізації системи аналізу ризиків є очевидною, зважаючи на специфіку діяльності підприємства і інформацію яка зберігається(персональна інформація, діагнози, історія хвороби, база електронних рецептів тощо) а також можливу кримінальну відповідальність за розголошення деяких видів інформації, можна прийти до висновку, що цінність інформації є набагато вищою за вартість проекту.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Вимоги щодо приміщення та робочих місць

Згідно з ДСанПІН 3.3.2.007-98Об'ємно-планувальні рішення будівель та приміщень для роботи з ВДТ ЕОГМ і ПЕОМ мають відповідати вимогам цихПравил. Розміщення робочих місць з ВДТ ЕОМ і ПЕОМупідвальнихприміщеннях, на цокольних поверхах заборонено. Площа не одне робоче місцемає становитинеменшеніж 6,0 м2, а об'єм не менше ніж 20,0 м3. Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення відповідно до СНиП II-4-79.

Вимоги безпеки до робочих місць працівників з екранними:

1. Робочі місця працівників з екранними пристроями мають бути спроектовані так і мати такі розміри, щоб працівники мали простір для зміни робочого положення та рухів.

2. Для забезпечення безпеки та захисту здоров’я працівників усе випромінювання від екранних пристроїв має бути зведене до гранично допустимого рівня (вплив на людину факторів довкілля - шуму, вібрації, забруднювачів, температури тощо, який не спричиняє соматичних або психічних розладів, а також змін стану здоров’я, працездатності, поведінки, що виходять за межі пристосувальних реакцій) з погляду безпеки та охорони здоров’я працівників.

3. Організація робочого місця працівника з екранними пристроями має забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним, антропологічним, психофізіологічним вимогам, а також характеру виконуваних робіт.

4. Освітлення робочого місця працівника з екранними пристроями має створювати відповідний контраст між екраном і навколишнім середовищем (з урахуванням виду роботи) та відповідати вимогам ДСанПІН 3.3.2.007-98.

5. Мікроклімат виробничих приміщень з робочими місцями працівників з екранними пристроями має підтримуватись на постійному рівні та відповідати

вимогам Санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 42 (далі - ДСН 3.3.6.042-99).

6. Робочий стіл або робоча поверхня повинні бути достатнього розміру та мати поверхню з низькою відбивною здатністю, допускати гнучкість під час розміщення екрана, клавіатури, документів і відповідного устаткування.

7. Робоче крісло має бути стійким і дозволяти працівнику з екранними пристроями легко рухатися та займати зручне положення. Сидіння має регулюватися по висоті, спинка сидіння - як по висоті, так і по нахилу.Слід передбачати підніжку для тих, кому це необхідно для зручності.

Мінімальні вимоги безпеки під час роботи з екранними пристроями:

1. Щодня перед початком роботи необхідно очищати екранні пристрої від пилу та інших забруднень.

2. Після закінчення роботи екранні пристрої слід відключати від електричної мережі.

3. У разі виникнення аварійної ситуації необхідно негайно відключити екранний пристрій від електричної мережі.

4. Не допускається:

виконувати технічне обслуговування, ремонт і налагодження екранних пристроїв безпосередньо на робочому місці працівника під час роботи з екранними пристроями;

відключати захисні пристрої, самочинно проводити зміни у конструкції та складі екранних пристроїв або їх технічне налагодження;

працювати з екранними пристроями, у яких під час роботи виникають нехарактерні сигнали, нестабільне зображення на екрані та інші несправності.

5. Під час виконання робіт операторського типу, пов’язаних з нервово-емоційним напруженням, у приміщеннях під час роботи з екранними пристроями, на пультах і постах керування технологічними процесами та в інших приміщеннях мають дотримуватися оптимальні умови мікроклімату відповідно до вимог ДСН 3.3.6.042-99.

Мінімальні вимоги безпеки до екранних пристроїв:

1. Екранні пристрої не мають бути джерелом ризику для працівників.

2. Усе випромінювання, за винятком видимої частини електромагнітного спектра, має бути зведене до незначного рівня з погляду безпеки і охорони здоров’я працівників.

3. Символи на екранних пристроях мають бути чіткими, відповідного розміру. Між символами і рядками символів має бути належна відстань.

4. Зображення на екрані має бути стабільним, без миготінь або інших видів нестабільності.

5. Яскравість та/або контрастність символів має легко регулюватися працівником під час роботи з екранними пристроями, а також швидко адаптуватися до навколишніх умов.

6. Вибираючи екрани, слід надавати перевагу таким екранам, які легко та вільно повертаються і нахиляються відповідно до потреби працівника.

7. За необхідності може використовуватись окрема підставка або регульований стіл для розміщення екрана.

8. Екран не має відблискувати або відбивати світло, щоб не викликати дискомфорту у працівника під час роботи з екранними пристроями.

9. Вибираючи клавіатуру, слід надавати перевагу такій клавіатурі, яка відкидається і є автономною (відокремленою від екрана), щоб працівник міг вибрати зручну робочу позу й уникнути втоми рук (кисті і верхньої частини руки).

10. Поверхня клавіатури має бути матовою, щоб уникнути віддзеркалювання. Розташування клавіш і самі клавіші мають полегшувати роботу із клавіатурою. Позначення клавіш повинно бути достатньо контрастним і розбірливим.

11. Устаткування, яке входить до робочої станції, не має виділяти надлишкового тепла, що може спричинити незручності працівникам під час роботи з екранними пристроями.

12. Під час розробки, вибору, замовлення та модифікації програмного забезпечення, а також під час розробки завдань, що передбачають використання устаткування з екранними пристроями, роботодавець має керуватися таким програмним забезпеченням, яке відповідає розв’язуваним завданням і є простим у використанні, а де необхідно - адаптованим до рівня знань і досвіду працівника.

Робоче приміщення, у якому проходило дослідження методів підвищення ефективності управління ризиками інформаційної безпеки підприємства, має відповідати вимогам щодо охорони праці при організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ВДТ).

Дане приміщення має 3 робочих місця. Розглянемо відповідність характеристик робочого місця нормативним. Для цього зведемо основні вимоги до організації робочого місця з і відповідні фактичні значення для робочого місця, за яким виконується робота, у табл. 6.1.

Робоче приміщення та місце відповідає вимогам щодо охорони праці при організації роботи з ВДТ електронно-обчислювальних машин.

Таблиця 6.1 — Характеристики робочого місця

Параметр	Позначення	Величина
Довжина, м	A	5
Ширина, м	B	4
Висота, м	H	3
Кількість робочих місць	N	3
Площа, м2	S	20
Об’єм, м3	V	60

Відповідно до ДСН 3.3.6.042-99 роботи, що виконуються користувачами ЕОМ, відносяться до легких фізичних робіт – категорії Іа. У виробничих

приміщеннях на робочих місцях з ВДТ мають забезпечуватись оптимальні значення параметрів мікроклімату.

Згідно ДБН В.2.5-28:2018 приміщення, що розглядається, повинне мати природне і штучне освітлення.

Денне (природне) освітлення приміщення відбувається за системою однобічного бічного освітлення. Природне світло проникає у приміщення через три світлові прорізи (віконні отвори), які мають регулювальні пристрої для відкривання. Також наявні штори (жалюзі) з можливістю захисту працюючих від прямого попадання сонячних променів і регулювання рівня освітленості в приміщенні. Вікна приміщення орієнтовані на північний схід. Оскільки будинок розташований у відносній віддаленості від прилеглих будівель, то які небудь перешкоди природному освітленню розглянутого приміщення відсутні.

Всередині приміщення стіни обклеєні світлими шпалерами, стеля побілена (переважає білий колір), у якості підлогового покриття використаний лінолеум світло-жовтого кольору.

Наявність постійного шуму в робочій зоні призводить до розладу центральної нервової системи і до таких захворювань як неврози, однак фактичний обмірюваний рівень шуму в робочій зоні склав 43 дБА, що задовольняє нормативному рівню шуму (не повинен перевищувати 50 дБА), тому додаткових заходів по поліпшенню цього фактору не потрібно.

Проаналізуємо стан електробезпеки в робочому приміщенні:

— всі прилади в кабінеті використовують напругу 220 В;
— електропроводка захована і ізольована від працівників спеціальним коробом;
— всі робочі місця з ПЕОМ використовують спільні розетки по 220 В;
— споживачі електроенергії — 3 ПЕОМ у вигляді ноутбуків;
— відносна вологість повітря – 60%, температура повітря +22 °С - +24 °С, струмопровідний пил і хімічно активні речовини в повітрі відсутні;

Проаналізувавши наведене вище, можемо сказати, що кабінет відноситься до приміщень без підвищеної електронебезпеки.

ПЕОМ, що використовуються в даному кабінеті підключаються до трифазної мережі і мають захисне занулення (за допомогою окремого захисного нульового провідника). Корпуси ВДТ та принтера виготовлені з пластику і не являються струмопровідними. Щодо корпусів самих ПЕОМ, вони виготовлені зі струмопровідного матеріалу, крім передньої панелі, що виготовлена з пластику.

При виконанні робіт по ремонту і обслуговуванню ПЕОМ обслуговуючий персонал зобов'язаний керуватися “Правилами техніки безпеки при експлуатації електроустановок споживачами". До роботи не допускаються особи, які не пройшли навчання з техніки безпеки.

Джерелом електромагнітного випромінювання в сучасному офісі є візуальні дисплейні термінали. Нормування електромагнітного випромінювання ВДТ а здійснюється згідно НПАОП 0.00-7.15-18 “Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями”.

6.2.1 Основні положення про надзвичайні ситуації

Надзвичайна ситуація (НС) – обстановка на окремій території чи суб’єкті господарювання на ній або водному об’єкті, яка характеризується порушенням нормальних умов життєдіяльності населення, спричинена катастрофою, аварією, пожежею, стихійним лихом, епідемією, епізоотією, епіфітотією, застосуванням засобів ураження або іншою небезпечною подією, що призвела (може призвести) до виникнення загрози життю або здоров’ю населення, великої кількості загиблих і постраждалих, завдання значних матеріальних збитків, а також до неможливості проживання населення на такій території чи об’єкті, провадження на ній господарської діяльності. Основними причинами виникнення надзвичайних ситуацій в Україні є:

— надзвичайне техногенне навантаження території;
— значний моральний та фізичний знос основних виробничих фондів більшості підприємств України;
— погіршення матеріально-технічного забезпечення, зниження виробничої і технологічної дисципліни;

— незадовільний стан збереження, утилізації та захоронення високотоксичних, радіоактивних та побутових відходів;

— ігнорування економічних факторів, вимог, стандартів;

Недостатня увага керівників відповідних органів державного управління до проведення комплексу заходів, спрямованих на запобігання надзвичайним ситуаціям природного і техногенного характеру та зниження їх наслідків; – відсутність сучасних систем управління небезпечними процесами; – низька професійна підготовка персоналу та населення до дій в екстремальних умовах; – дефіцит кваліфікованих кадрів; – низький рівень застосування прогресивних ресурсозберігаючих і екологобезпечних технологій.

Класифікаційна ознака НС – технічна або інша характеристика небезпечної події, що зумовлює виникнення обстановки, яка визначається як надзвичайна ситуація. Порогове значення класифікаційної ознаки НС – визначене в установленому порядку значення технічної або іншої характеристики конкретної аварійної ситуації, перевищення якого відносить ситуацію до рангу надзвичайних і потребує відповідного рівня реагування.

Зона надзвичайної ситуації – окрема територія, акваторія, де сталася надзвичайна ситуація.

Аварія – небезпечна подія техногенного характеру, що спричинила ураження, травмування населення або створює на окремій території чи території суб’єкта господарювання загрозу життю або здоров’ю населення та призводить до руйнування будівель, споруд, обладнання і транспортних засобів, порушення виробничого або транспортного процесу чи спричиняє наднормативні, аварійні викиди забруднюючих речовин та інший шкідливий вплив на навколишнє природне середовище.

Катастрофа – велика за масштабами аварія чи інша подія, що призводить до тяжких наслідків.

Небезпечна подія – подія, у тому числі катастрофа, аварія, пожежа, стихійне лихо, епідемія, епізоотія, епіфітотія, яка за своїми наслідками становить

загрозу життю або здоров’ю населення чи призводить до завдання матеріальних збитків.

Надзвичайна ситуація техногенного характеру – порушення нормальних умов життя та діяльності людей на окремій території чи об'єкті на ній або на водному об'єкті унаслідок транспортної аварії (катастрофи), пожежі, вибуху, аварії з викиданням (загрозою викидання) небезпечних хімічних, радіоактивних і біологічно небезпечних речовин, раптового руйнування споруд; аварії в електроенергетичних системах, системах життєзабезпечення, системах телекомунікацій, на очисних спорудах, у системах нафтогазового промислового комплексу, гідродинамічних аварій тощо

Надзвичайна ситуація природного характеру – порушення нормальних умов життя та діяльності людей на окремій території чи об'єкті на ній або на водному об'єкті, пов'язане з небезпечним геофізичним, геологічним, метеорологічним або гідрологічним явищем, деградацією ґрунтів чи надр, пожежею у природних екологічних системах, зміною стану повітряного басейну, інфекційною захворюваністю та отруєнням людей, інфекційним захворюванням свійських тварин, масовою загибеллю диких тварин, ураженням сільськогосподарських рослин хворобами та шкідниками тощо.

Надзвичайна ситуація соціального характеру – порушення нормальних умов життя та діяльності людей на окремій території чи об'єкті на ній або на водному об'єкті, спричинене протиправними діями терористичного і антиконституційного спрямування, або пов'язане із зникненням (викраденням) зброї та небезпечних речовин, нещасними випадками з людьми тощо.

Надзвичайна ситуація воєнного характеру – порушення нормальних умов життя та діяльності людей на окремій території чи об'єкті на ній або на водному об'єкті, спричинене застосуванням звичайної зброї або зброї масового ураження, під час якого виникають вторинні чинники ураження населення, що її визначають в окремих нормативних документах.

6.2.2 Планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації

При виникненні НС організовується надзвичайне управління, яке складається з чотирьох стадій ліквідації її наслідків.

Перша стадія вжиття екстрених заходів. Мета – задіяти механізм надзвичайного управління і вчасно зреагувати на НС. Основні завдання початкової стадії: встановлення факту НС, попередня оцінка обстановки в зоні лиха і масштабів наслідків, мобілізація і визначення оперативних завдань органам надзвичайного управління, віддача розпоряджень на залучення мобільних сил пожежної охорони, швидкої медичної допомоги, охорони громадського порядку й інших служб для допомоги потерпілим, сприяння місцевим органам влади в організації рятувальних робіт і локалізації зони НС власними силами; інформування населення та керівних органів управління про НС і вжиті заходи. Тривалість початкової стадії – 1-10 годин.

Друга стадія оволодіння ситуацією й організації механізму надзвичайного управління у зоні НС. Завдання: детально оцінити обстановку, терміново прийняти обґрунтоване рішення й уточнити план ліквідації наслідків НС; розрахувати необхідні сили і засоби, ресурси для всього комплексу робіт у зоні лиха, організувати чітку взаємодію всіх залучених сил і аварійних служб. Тривалість 2-ї стадії – від кількох годин до кількох діб.

Третя– основна і визначальна стадія. Мета – перебороти надзвичайний характер ситуації: відновити безпеку населення в зоні НС, ліквідувати загрозу життю і здоров'ю всім потерпілим, створити мінімально необхідні умови для життєдіяльності населення, що залишилося. Завдання: розгортання в найкоротший термін рятувальних робіт на всіх постраждалих об'єктах зони НС, надання допомоги потерпілим для захисту їхнього життя, здоров'я і підтримка життєздатності в екстремальних умовах; евакуація потерпілих із зони НС та їх життєзабезпечення; термінове проведення аварійно-відновлювальних робіт на системах водо-, тепло-, газо-, електропостачання і зв'язку в зоні НС. Тривалість – кілька діб – кілька тижнів.

Четверта стадія – відновлення, тобто економічна, соціальна, культурна й екологічна реабілітація зони НС. Органи надзвичайного управління вичерпали свою роль і передають функції постійної дії місцевим органам управління. 26 Розробляється спеціальна програма з черговістю комплексу заходів для реабілітації зони НС.

Висновки до розділу

В даному розділі було проведено ознайомлення з діючим законодавством про охорону праці та проаналізовано основні проблеми, що можуть виникнути під час роботи працівника. Було виділено основні вимоги до приміщення, мікроклімату в приміщенні, освітлення та основних ергономічних характеристик. Також було ознайомлено з основними видами надзвичайних ситуацій, їх класифікацією а також з планування заходів цивільної безпеки у випадку її настання.

7 ЕКОЛОГІЯ

7.1 Енергозбереження і його роль у вирішенні екологічних проблем.

Енергозбереження стосується зменшення споживання енергії за рахунок використання меншої кількості енергетичних послуг. Енергозбереження відрізняється від енергоефективності, яке стосується використання меншої кількості енергії за ту саму послугу. Наприклад, менше користуватись авто — заощадження енергії, а перейти на авто з меншою витратою палива, або на електромобіль — енергоефективність. Але і енергозбереження, і енергоефективність є техніками зменшення використання енергії.

Для заохочення споживачів зменшувати споживання енергії деякі країни запровадили енергетичні або вуглецеві податки. Вуглецеві податки можуть спричиняти зміну споживання енергії з викопного палива на атомну енергетику та інші альтернативи, які мають свої обмеження та наслідки впливу на довкілля.

Натомість, енергетичні податки спрямовано на загальне зниження споживання енергії (будь-якого походження), і відповідно на зниження більшого спектру негативних наслідків для довкілля, спричинений виробництвом енергії. Наприклад, в США штат Каліфорнія застосовує прогресивну шкалу енергетичного податку, коли кожен споживач має встановлений рівень споживання енергії, для якого податок низький. Але у разі перевищення зазначеної межі, податок зростає експоненціально. Такі програми спрямовані на захист біднішого населення і створення більшого податкового тягаря на господарства з високим рівнем споживання енергії.

З обмеженнями, але прикладом такого енергетичного податку в Україні може бути ціна на газ для населення (залежить від річного обсягу споживання). Обмеження викликані тим, що прогресивна шкала ціни була встановлена не як енергетичний податок, а для регулювання дотацій.

Основними напрямками і способами енергозбереження за видами енергії є:

Економія електроенергії:

— Оптимізація освітлення

— максимальне використання денного світла (збільшення кількості, площі та прозорості вікон);
— збільшення відбивної здатності (світлі стіни та стелі);
— оптимальне розміщення джерел штучного світла (місцеве, направлене освітлення);
— використання освітлювальних приладів лише за необхідністю;
— підвищення світловіддачі наявних джерел світла (заміна люстр, відбивачів тощо);
— використання приладів управління освітленістю (давачі руху, акустичні датчики, давачі освітленості, таймери, дистанційне керування, регулятори яскравості);
— запровадження автоматичної системи диспетчерського управління зовнішнім освітленням
— установка інтелектуальних розподілених систем управління освітленням.

Електропривід:

— оптимальний підбір потужності електродвигуна;
— використання частотно-регульованого приводу.

Заходи по зниженню втрат тепла та підвищенню ефективності систем теплопостачання:

— джерело теплопостачання
— зменшення витрат енергії та тепла на власні потреби;
— використання сучасного обладнання з вищим ККД теплогенерації, напр. конденсаційні котли теплові насоси;
— використання вузлів обліку теплової енергії;
— використання ко- і три- генерації.
— теплові мережі
— ізоляція мереж для зниження втрат тепла у довкілля;
— скорочення шляху теплоносія від виробника до споживача теплової енергії (напр., міні-котельня у будинку)
— оптимізація гідравлічних режимів тепломереж;
— зменшення протікань.

— споживачі
— належна ізоляція опалюваних приміщень;
— використання систем місцевого регулювання опалювальних приладів;
— переведення будинків до режиму нульового споживання тепла для опалення (температура всередині підтримується за рахунок внутрішнього тепловиділення (рекуперація) та гарної ізоляції (вікна з аерогелем));
— використання вузлів обліку теплової енергії.

Економія води:

— встановлення приладів обліку використання води;
— використання води лише коли дійсно необхідно;
— встановлення зливних бачків, які мають функцію вибору сили зливу;
— встановлення автоматичних регуляторів витрат води, аераторів, сенсорних давачів.

Економія газу:

— підбір оптимальної потужності котла та насосу (наприклад, якщо є пікове, але нечасте, навантаження, можливо краще замість одного придбати два котла меншої потужності, один з яких працюватиме постійно, а другий включатиметься за потреби);
— належна теплоізоляція опалюваних приміщень, ефективні радіатори;
— використання на газових плитах посуду з широким пласким дном, підігрів лише необхідної кількості їжі та води;
— за можливості перехід на альтернативне опалення (напр., котли на біомасі, сонячні колектори, теплові насоси).
— правильне використання будівельної ізоляції.

Споживачі часто погано проінформовані про використання енергії енергоефективними продуктами. Зусилля для пошуку шляхів збереження енергії часто забирають багато часу та коштів, а поряд багато дешевшої продукції і технологій, які споживають викопне паливо. Уряди деяких країн та неурядові організації намагаються зменшити складність вибору за рахунок екологічних

маркувань, які дають змогу легко побачити різницю у енергоспоживанні при пошуку товару.

Для того, щоб надати інформацію і заохотити людей інвестувати кошти, час та зусилля у енергозбереження, необхідно розуміти і адресувати їх актуальні проблеми. Наприклад, деякі торгові мережі вважають, що яскраве освітлення стимулює покупки. Однак, дослідження проблем здоров'я показали, що надмірне освітлення, звичайне на багатьох робочих місцях та магазинах, насправді стимулює головний біль, стрес, підвищує артеріальний тиск, втому та збільшує кількість помилок. Дослідження показали, що збільшення природного денного світла збільшило продуктивність працівників, і одночасно зменшило споживання енергії.

При виборі нових пристроїв потрібно надавати перевагу приладам з меншим енергоспоживанням, як в активному режимі, так і у режимі стенд-бай, використовувати режим автоматичне вимкнення, підігрівати лише стільки води/їжі, скільки плануєте використати, не залишати включеними в мережу зарядні пристрої для мобільних приладів (телефонів, планшетів, нетбуків тощо); намагайтеся не використовувати подовжувачі, а якщо це необхідно — використовуйте якісні та з більшим перерізом (при малому провід більше гріється, а отже менше корисне використання енергії). Також використовувати енергоощадні, насамперед, світлодіодні, а ззовні, натрієві лампи.

7.2 Статистика екологічних показників

Система показників охорони навколишнього середовища, яка діє в Україні, грунтується на розробленій у 70-ті роки системі статистичної звітності, що стосується навколишнього середовища. Головним завданням цієї галузі статистики стало забезпечення органів управління та планування інформацією, яка була необхідна для визначення стратегії та тактики природокористування і охорони навколишнього середовища в країні, заходів з регулювання впливу господарської діяльності на довкілля.

Система показників стану навколишнього середовища безпосередньо пов'язана з чинною системою статистичної звітності. Створена форма

статистичної звітності забезпечила збір даних про найбільш гострі проблеми, пов'язані з антропогенним впливом на окремі складові навколишнього середовища і поклала основу для побудови системи показників, яка мала виражений по елементний характер і складалася з таких розділів:

— показники стану, використання і охорони водних ресурсів;
— показники забруднення, охорони і стану атмосферного повітря;
— показники стану, використання і охорони земельних ресурсів;
— показники стану, використання і охорони лісових ресурсів;
— показники наявності, охорони і використання тваринного та рослинного світу;
— показники охорони надр, наявності і раціонального використання мінеральних ресурсів;
— показники наявності, стану і охорони заповідних територій;
— показники утворення, видалення і утилізації промислових відходів;
— показники утворення побутових відходів і охорони навколишнього середовища від їх забруднення;
— показники наявності, стану і використання основних фондів природоохоронного призначення.

В більшості розділів можна виділити шість груп показників:

— наявність та склад забруднень;
— показники антропогенного впливу, що викликає ті чи інші зміни навколишнього середовища;
— природоохоронні заходи;
— показники якісного стану або ступеня забруднення (в регіонах і населених пунктах);
— витрати на охорону природи;
— ефективність природоохоронних витрат.

Міжнародне співтовариство на даному етапі розглядає показники стану навколишнього середовища як комплексний інструментарій для виміру та

репрезентації еколого-економічних тенденцій у країні. Виходячи з цих позицій, можна виділити чотири основні типи показників:

показники сучасного екологічного стану, які визначають чинні екологічні параметри;

показники впливу або тиску, які відображають антропогенний вплив на навколишнє середовище;

показники, що регулюють вплив на навколишнє середовище, і за допомогою яких визначається, як різні агенти реагують на специфічний вплив;

показники якісного стану або ступеня забруднення (в регіонах і населених пунктах).

ВИСНОВКИ

У магістерській роботі здійснено дослідження методів підвищення ефективності управління ризиками інформаційної безпеки підприємства та вибір і обґрунтування найоптимальніших методів для некомерційних комунальних підприємств у сфері охорони здоров’я.

Зокрема, розглянуто структуру інформаційної безпеки підприємства, досліджено поняття та види загроз у інформаційній безпеці, проаналізовано загальні положення про ризики інформаційних систем та управління ними.

Інформаційні системи та кібербезпеку у нашому дослідженні розглянуто крізь призму системного підходу до управління бізнесом. Також здійснено структурний аналіз інформаційного середовища а саме систему управління ризиками інформаційної безпеки підприємства, охарактеризовано методи аналізу ризиків інформаційної безпеки, розглянуто методи та стандарти аналізу інформаційної системи. Усе це стало теоретико-методологічною основою для обґрунтування реалізації системи управління ризиками кібербезпеки для некомерційного комунального підприємства у сфері охорони здоров’я на основі стандартів ISO/IEC TR 13335.

В розділі «Структура інформаційної безпеки» містяться загальні відомості про інформаційну безпеку, а також про вразливості інформаційної безпеки та відомі ризики. Поверхнево розглянуто історичні передумови виникнення сучасних методик управління ризиками.

В розділі «Структура інформаційної системи підприємства, ризики та загрози» розглянуто сучасні підходи до управління бізнесом та пов’язані з цим характерні ризики та загрози інформаційній безпеці підприємства.

Висновки, зроблені у результаті дослідження ризиків, є вхідними даними для визначення стратегії ризик-менеджменту. Під стратегією розуміється цілісне (системне) і перспективне (відносно тривале у часі) бачення мети, завдань, напрямків управління ризиками, а також вибір відповідних методів, засобів та планування необхідних ресурсів (матеріальних, кадрових тощо).

Вплив на ризики, по суті, є основою ризик-менеджменту. Вплив здійснюється щодо ризиків, виявлених у процесі дослідження бізнес-середовища (наприклад, інформаційного середовища підприємства на предмет уразливості). Здійснення впливу на ризики зазвичай відбувається у межах окресленої стратегії. Варто розуміти, що стратегія є орієнтиром, а не докладним планом конкретних дій, а відтак, розробка стратегії управління ризиками не замінює прийняття рішень при безпосередньому впливі на ризики.

Метою впливу є приведення показників існуючих ризиків до їхніх мінімально можливих значень, відповідно до умов. Після досягнення зазначеної мети, а також за умови стартових задовільних показників, виявлених ще на етапі дослідження, необхідно на постійній основі здійснювати контроль за змінами.

У розділі «Методи аналізу ризиків інформаційної системи підприємства» міститься характеристика сучасний методів аналізу та управління ризиками інформаційної безпеки, а також їх відповідність сучасним міжнародним стандартам. Одну з методик було застосовано до об’єкту дослідження – некомерційного комунального підприємства, визначивши основні вразливості, що дозволило класифікувати їх та визначити пріоритетні напрями роботи в сфері протидії загрозам інформаційної безпеки підприємств даного типу.

Зокрема, в підрозділі 3.1 досліджено найпоширеніші методи аналізу ризику інформаційних систем: якісні, кількісні і змішані, порівняно їх переваги та недоліки, а також доцільність використання. У підрозділі 3.2 описано стандарти і методи оцінки ризиків, а в підрозділі 3.3 на основі стандарту ISO/IEC TR 13335 реалізовано систему управління ризиками безпеки некомерційного комунального підприємства – закладу охорони здоров’я.

В спеціальній частині роботи виконано пов’язане з управлінням ризиками індивідуальне завдання.

БІБЛІОГРАФІЯ

1. Courtney, R. 1977. Securityrisk assessmentin electronicdata processing. AFIPS Conference Proceedings National ComputerConference 46, 97-104.

2. Government of Canada, CommunicationsSecurityEstablishment. 1999. Threatand Risk Assessment Working Guide.

3. Kendall, K. Lyytinen, K., DeGross, J. IFIP Transactions A8 TheImpact of ComputerSupported Technologies onInformation Systems Development. Amsterdam: North-Holland, 43-60.

4. Management of Federal InformationResources, Office of Managementand Budget 1996. OMB Circular A-130. Washington.

5. Meritt, W.J. 1998. RiskManagement. 21th NISSC (National Information Systems Security Conference). Arlington, Virginia.

6. Ozier, W. 1997. Issuesin Qualitative risk analysis. Data Pro Report, August. NewYork: McGraw-Hill.

7. Parker, D. 1976. Crimeby Computer. NewYork: Chas Scribners Sons.

8. Sumner, M. 1992. Theimpact of Computer Assisted Software Engineering on Systems Development.

9. U.S. Department of Commerce, National Bureau of Standards, 1979.Guideline for Automatic Data Processing Risk Analysis, Federal Information Processing Standards Publication FIPS 65.

10. Whitman M.E., Mattord H.J., Readings and Cases in the Management of Information Security, Thomson Course Technology, Boston 2006, s. 52.

11. Абакумов В. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/5355/Informatsiina%20bezpeka%20pidpryiemnytstva%20yak%20obiekt%20administratyvno_pravovoi%20okhorony_Abakumov_2012.pdf?sequence=1&isAllowed=y.

12. Арапова А. Система управління ризиками як необхідна складова забезпечення кібербезпеки. URL:

http://repository.mdu.in.ua/jspui/bitstream/123456789/658/1/kiberbezpeka_2018.pdf#page=89.

13. Архипов О. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Архипов, А. Скиба // Захист інформації. – 2013. – Т. 15, № 4. – С. 366–375.

14. Баранов В. Кібербезпека у 2018 році: новий виклик для бізнесу, необхідність чи побажання? URL: http://yur–gazeta.com/publications/practice/informaciyne–pravo–telekomunikaciyi/kiberbezpeka–u–2018–roci–noviy–viklik–dlya–biznesu–neobhidnist–chi–pobazhannya.html.

15. Борсуковський Ю. Базові напрямки забезпечення кібербезпеки державного та приватного секторів / Ю. Борсуковський, В. Бурячок, В. Борсуковська // Сучасний захист інформації. – 2017. – № 2 (30). – С. 85–89.

16. Братюк В. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні / В. Братюк // Актуальні проблеми економіки. – 2015. – № 9. – С. 421–427.

17. Бучик С. Методика оцінювання інформаційних ризиків в автоматизованій системі / С. Бучик, С. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. – 2015. – Вип. 11. – С. 33–43.

18. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість у контексті вдосконалення інформаційного законодавства / М. Василенко // Юридичний вісник. – № 3. – 2018. – С. 17–24.

19. Верескун М. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М. Верескун // Економіка і організація управління. – 2014. – Вип. 1–2. – С. 54–60.

20. Віннікова І. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними / І. Віннікова, С. Марчук // Східна Європа: економіка, бізнес та управління. – 2018. – № 5. – С. 110–114.

21. Власюк Ю., Архипов О. Економічні аспекти кібербезпеки. URL: https://ela.kpi.ua/bitstream/123456789/17247/1/Vlasiuk.pdf.

22. Войнаренко П., Рзаєв Г., Рзаєва Т. Інформаційна безпека підприємства у динамічному ринковому середовищі. URL: http://elar.khnu.km.ua/jspui/bitstream/123456789/1889/1/VOYNARENKO.pdf.

23. Волкова В., Васютенко М. Визначення витрат на забезпечення інформаційної безпеки підприємства на засадах математичного моделювання. URL: http://www.vestnikdnu.com.ua/archive/201482/222.html.

24. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. URL: http://zt.knteu.kiev.ua/files/2018/03(98)/10.pdf.

25. Глушак В., Новіков О. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника. URL: https://ela.kpi.ua/bitstream/123456789/6875/1/09_Glush.pdf.

26. Гнатюк В. Аналіз дефініцій поняття "інцидент" та його інтерпретація у кіберпросторі / В. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 3. – С. 175–180.

27. Гончар С. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом / С. Гончар // Захист інформації. – 2014. – Т. 16, № 1. – С. 40–46.

28. Горяна О. Система управління інформаційною безпекою. URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1876/SUIB.pdf?sequence=1&isAllowed=y.

29. Грінченко Є., Колмик О. Методи управління інформаційними ризиками. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/5853/Metody%20upravlinnia%20informatsiinymy%20ryzykamy_Grinchenko_Kolmyk_2018.pdf?sequence=1.

30. Довгань О. Корпоративна культура кібербезпеки суб’єктів наукової та науково-технічної діяльності / О. Довгань, А. Тарасюк // Інформація і право. – № 2 (25). – 2018. – С. 51–61.

31. Дрожанова О., Ступак О. Кібербезпека в цифровій економіці: соціально-філософський аспект. URL: http://eir.nuos.edu.ua/xmlui/bitstream/handle/123456789/2402/Drozhanova2.pdf?sequence=1.

32. Євтушевська О. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту. URL: http://zt.knteu.kiev.ua/files/2015/5–6%20(82–83)/18.pdf.

33. Завгородня М. Можливості та ризики використання цифрових технологій у промисловості. URL: https://ir.kneu.edu.ua/bitstream/handle/2018/31551/ZE_2019_55.pdf?sequence=1&isAllowed=y.

34. Збожинський С. Інформаційна безпека під час застосування цифрових технологій. URL: http://yur–gazeta.com/publications/practice/zahist–intelektualnoyi–vlasnosti–avtorske–pravo/informaciyna–bezpeka–pid–chas–zastosuvannya–cifrovih–tehnologiy.html.

35. Зубко О. Використання методики факторного аналізу інформаційних ризиків в процесі забезпечення кібербезпеки малих комерційних підприємств. Дипломна робота магістра / О. Зубко. – Дніпро, 2018. – 115 с.

36. Зубок М. Інформаційна безпека в підприємницькій діяльності. Підручник / М. Зубок. – Київ, 2015. – 216 с.

37. Іванова В. Інформаційна безпека як підсистема в системі економічної безпеки підприємства. URL: http://eprints.kname.edu.ua/38599/1/67–71.pdf.

38. Ігнатьєва І. Функціональні методи оцінки ризику кібербезпеки. Дипломна робота магістра / Ігнатьєва І. – Дніпро, 2018. – 106 с.

39. Ілляшенко О. Методи і засоби забезпечення виконання вимог до кібербезпеки систем на програмовнійлогіці. URL: http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/38543/5/avtoreferat_2018_Illiashenko_Metody_i_zasoby.pdf.

40. Казакова Н., Вавілов Є. Автоматизація процесу адаптації інформаційних систем до інцидентів інформаційної безпеки. URL:

http://dspace.oneu.edu.ua/jspui/bitstream/123456789/1501/1/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F%20%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%83%20%D0%B0%D0%B4%D0%B0%D0%BF%D1%82%D0%B0%D1%86%D1%96%D1%97%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%20%D0%B4%D0%BE%20%D1%96%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D1%96%D0%B2%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8.pdf.

41. Качан О. Інформаційна безпека підприємства в умовах глобалізації. URL: https://conf.ztu.edu.ua/wp–content/uploads/2017/09/234.pdf.

42. Кириленко А., Бабинюк О. Кібербезпека на захисті бізнесу. URL: https://ir.kneu.edu.ua/bitstream/handle/2018/31417/ZE_2019_118.pdf?sequence=1.

43. Кіпчарська Я. Методичні засади забезпечення інформаційної безпеки поліграфічного підприємства. URL: http://nz.uad.lviv.ua/static/media/4–45/13.pdf.

44. Ключник Т. Кібербезпека як новий виклик сучасності. URL: http://elar.naiau.kiev.ua/bitstream/123456789/7055/1/%D0%90%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%20%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8%20%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B8_p052-053.pdf.

45. Ковальов І. Оцінка ризиків інформаційної безпеки з використанням алгоритму нечіткої кластеризації k-середніх. Дипломна робота магістра / І. Ковальов. – Дніпро, 2018. – 78 с.

46. Кожедуб Ю. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST. URL: https://ela.kpi.ua/bitstream/123456789/23949/1/ITS2017.5.2(9)_09.pdf.

47. Козак Н., Цимбал П., Варшавець Я. Деякі аспекти виявлення і попередження інцидентів кібербезпеки. URL: http://ir.nusta.edu.ua/jspui/bitstream/123456789/2339/1/2219_IR.pdf.

48. Корченко О. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія / О. Корченко, С. Казмірчук, Б. Ахметов. – Київ, 2017. – 435 с.

49. Крижанівський В. Безпека інформаційних систем. Конспект лекцій / В. Крижанівський. – Житомир, 2012. – 110 с.

50. Лисенко Ю. Модель ефективності IT-аутсорсингу в контексті розвитку інформаційних систем економічних об'єктів / Ю. Лисенко, Є. Бізянов // Проблеми економіки. – 2013. – № 2. – С. 190–195.

51. Маркіна І., Дячков Д. Основи формування системи менеджменту інформаційної безпеки підприємства. URL: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/3092/1/piprp_2016_3%281%29__18.pdf.

52. Мельник М. О. Аналіз побудови моделі політики інформаційної безпеки підприємства / М. Мельник, Г. Нікітин, К. Мезенцева // Системи обробки інформації. – 2017. – Вип. 2. – С. 126–128.

53. Микитенко Т. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах / Т. Микитенко, І. Петровська, П. Рогов, А. Гаркуша // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2016. – № 2. – С. 24–31.

54. Мохор В., Бакалинський О., Цуркан В. Представлення оцінок ризиків інформаційної безпеки картою ризиків. URL: http://nbuv.gov.ua/j–pdf/inftech_2018_6_2_10.pdf.

55. Нашинець-Наумова А. Питання забезпечення економічної безпеки підприємства. URL: http://law.nau.edu.ua/images/Nauka/Naukovij_jurnal/2012/statji_n3_24_2012/Nashinec_Naumova_58.pdf.

56. Нехай В., Нехай В. Інформаційна безпека як складова економічної безпеки підприємств. URL: http://www.vestnik–econom.mgu.od.ua/journal/2017/24–2–2017/30.pdf.

57. Новікова А. Питання кібербезпеки у світі юриспруденції. URL: https://sud.ua/ru/news/publication/138379–pitannya–kiberbezpeki–u–sviti–yurisprudentsiyi.

58. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. URL: http://ibo.tneu.edu.ua/index.php/ibo/article/view/124/123.

59. Піляй А. Інформаційна безпека. Чи працює Політика ІБ у Вашій компанії? URL: https://legalitgroup.com/informaciyna–bezpeka–v–kompanii/.

60. Пузиренко О. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем / О. Пузиренко, С. Івко, О. Лаврут // Системи обробки інформації. – 2014. – Вип. 8. – С. 128–134.

61. Рудий Т. Засади захисту інформації в інформаційних системах підприємств / Т. Рудий, Л. Томаневич, О. Руда // Актуальні проблеми економіки. – № 2 (152). – 2014. – С. 551–557.

62. Савельєва Т., Панаско О., Пригодюк О. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства / Т. Савельєва, О. Панаско, О. Пригодюк // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2018. – Т. 1, № 4. – С. 81–89.

63. Сазонець О., Сіпайло Л. Інноваційна діяльність підприємств у контексті забезпечення інформаційної безпеки. URL: https://www.problecon.com/export_pdf/problems–of–economy–2015–3_0–pages–156_161.pdf.

64. Самедова Л. Ідентифікація поняття інформаційної безпеки в сучасних економічних умовах. URL: http://ep3.nuwm.edu.ua/11750/1/%D0%A1%D0%B0%D0%BC%D0%B5%D0%B4

%D0%BE%D0%B2%D0%B0_%D0%9B_%D0%A0%20%D0%B7%D0%B0%D1%85.pdf.

65. Северина С. Інформаційна безпека та методи захисту інформації / С. Северина // Вісник Запорізького національного університету. Економічні науки. – 2016. – № 1. – С. 155–161.

66. Сотниченко В. Інформаційна безпека як базова складова економічної безпеки телекомунікаційного підприємства. URL: http://www.dut.edu.ua/uploads/p_1010_25433567.pdf.

67. Твердохліб І. Управління інцидентами кібербезпеки на малих комерційних підприємствах. Дипломна робота магістра / І. Твердохліб. – Дніпро, 2018. – 132 с.

68. Цвілій О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою / О. Цвілій // Телекомунікаційні та інформаційні технології. – 2014. – № 2. – С. 73–79.

69. Чунарьова А. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп'ютеризованих системах / А. Чунарьова, І. Пархоменко, І. Сащук // Вісник Інженерної академії України. – 2014. – Вип. 2. – С. 138–142.

70. Шарина М., Володін В. Інформаційна складова економічної безпеки підприємства. URL: http://www.economy.nayka.com.ua/?op=1&z=5176.

71. методичні рекомендації з питань перетворення закладів охорони здоров'я з бюджетних установ у комунальні некомерційні підприємства https://moz.gov.ua/article/news/algoritm-avtonomizacii-medzakladu