Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)

спеціальність *Кібербезпека*
(код і назва спеціальності)

освітній рівень *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Функціональні методи оцінки ризику кібербезпеки***

Виконавець: студент ***6*** **курсу, групи** ***125м-16-1***

_____ ***Ігнатьєва Ірина Дмитрівна***
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	д.т.н., доц. Корнієнко В.І.		
розділів:			
спеціальний	ст. в. Галушко С.О.		
економічний	доц. Волотковська Ю.О.		
Рецензент			
Нормоконтроль	доц. Гусєв О.Ю.		

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., доц. _____ Корнієнко В.І.

«_____»_____2018 року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** ***Ігнатьєвій Ірині Дмитрівні***
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Функціональні методи оцінки ризику кібербезпеки***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від 26 грудня 2017 №2127-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *процес загальної оцінки ризику кібербезпеки функціональним методом на підприємствах України.*

Предмет досліджень *оцінка ризиків кібербезпеки функціональним методом.*

Мета НДР *підвищення кібербезпеки на підприємствах України за допомогою оцінки ризиків функціональним методом.*

Вихідні дані для проведення роботи *законодавство України та міжнародні стандарти у сфері інформаційної безпеки, наукові публікації вітчизняних та іноземних авторів, офіційні статистичні дані з інцидентів інформаційної безпеки, показники діяльності підприємства.*

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *полягає в аналізуванні ризиків кібербезпеки найбільш*

придатним функціональним методом та запобіганні ризиків в подальшому.

Практична цінність *розробка рекомендацій для вибору метода оцінки ризиків кібербезпеки, а також рекомендацій щодо запровадження методу на підприємстві.*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та бути поданим у вигляді, що дозволяє безпосереднє використання при прийнятті рішення з оцінки ризиків в процесі управління ризиками кібербезпеки на підприємстві.

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Аналіз стандартів управління ризиками інформаційної безпеки та методів оцінки ризиків, порівняння моделей прийняття рішень з інформаційної безпеки	01.12.2017 - 11.12.2017
Дослідження методів кількісної оцінки ризику та моделей аналізу ризиків кібербезпеки	11.12.2017 - 15.12.2017
Розробка методики прийняття рішень щодо вибору методу оцінки ризику інформаційної безпеки	18.12.2017 - 22.12.2017
Застосування обраного методу до об’єкта інформаційної діяльності	25.12.2017 - 29.12.2017
Визначення капітальних та експлуатаційних витрат на реалізацію запропонованих рекомендації із захисту інформації та довести економічну ефективність цих рекомендацій	05.01.2018 - 19.01.2018
Оформлення технічної документації дипломної роботи	12.01.2018 - 19.01.2018

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки оптимізації витрат на інформаційну безпеку через застосування запропонованої у дипломній роботі методики прийняття рішень.*

Соціальний ефект *дипломної роботи, як наслідок зменшення критичних ризиків, полягає у підвищенні впевненості клієнтів та працівників підприємства у його надійності.*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:
ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення».
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи (проекту) для студентів галузей знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Бабенко Т.В., Корнєєв М.В., Кручінін О.В., Тимофєєв Д.С.; Нац. гірн. ун-т. – Д: НГУ, 2016. – 45 с.
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи

Завдання видав _____ ст.вик. Галушко С.О.
(підпис) (прізвище, ініціали)

Завдання прийняла до виконання _____ ст. Ігнатьєва І.Д.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 30.11.2017

Термін подання дипломної роботи до ДЕК _____

РЕФЕРАТ

Пояснювальна записка: ___с., __ рис., __табл., __додатків,__ джерел.

Об’єкт дослідження: процес загальної оцінки ризику кібербезпеки функціональним методом на підприємствах України.

Мета роботи: підвищення кібербезпеки на підприємствах України за допомогою оцінки ризиків функціональним методом. Методи дослідження: порівняння, аналізування, моделювання, оцінка.

В спеціальній частині дана характеристика типового об’єкту інформаційної діяльності, до якого було застосовано вибраний метод оцінки ризиків. В роботі проаналізовано моделі вибору оптимальної системи захисту інформації та нормативно-правова база України, що регулює сфери інформаційної безпеки та кібербезпеки. Досліджено процес та моделі оцінки ризиків кібербезпеки. Запропоновані рекомендації щодо вибору методу та застосування його на практиці. В економічній частині було розраховано вартість інформаційних ресурсів підприємства, капітальні та експлуатаційні витрати на засоби захисту для зменшення ризику кібербезпеки. Практичне значення роботи полягає в застосуванні обраного методу оцінки ризику, а також розробці методики запобігання ризику кібербезпеки. Наукова новизна роботи полягає в розробці методики запобіганню ризиків інформаційної безпеки, що застосовує метод оцінки ризику.

Ключові слова: АНАЛІЗ РИЗИКІВ, МЕТОДИ ОЦІНКИ РИЗИКІВ, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, ВАРТІСТЬ ІНФОРМАЦІЙНОГО АКТИВУ, ЗАПРОВАДЖЕННЯ МЕТОДУ “КРАВАТКА-МЕТЕЛИК”.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., __ приложений, __источников.

Объект исследования: процесс общей оценки риска кибербезопасности функциональным методом на предприятиях Украины.

Цель работы: повышение кибербезопасности на предприятиях Украины при помощи оценки рисков функциональным методом.

Методы исследования: сравнение, анализ, моделирование, оценка.

В специальной части дана характеристика типичного объекта информационной деятельности, к которому было применено выбранный метод оценки рисков. В работе проанализированы модели выбора оптимальной системы защиты информации и нормативно-правовая база Украины, регулирующая сферы информационной безопасности и кибербезопасности. Исследован процесс и модели оценки рисков кибербезопасности. Предложены рекомендации по выбору метода и применение его на практике.В экономической части было рассчитано стоимость информационных ресурсов предприятия, капитальные и эксплуатационные затраты на средства защиты для уменьшения риска кибербезопасности. Практическое значение работы состоит в применении выбранного метода оценки риска, а также разработке методики предотвращения риска кибербезопасности. Научная новизна работы заключается в разработке методики предотвращения рисков информационной безопасности, применяя метод оценки риска при его оценке.

Ключевые слова: АНАЛИЗ РИСКОВ, МЕТОДЫ ОЦЕНКИ РИСКОВ, КИБЕРБЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УПРАВЛЕНИЕ РИСКАМИ, СТОИМОСТЬ ИНФОРМАЦИОННОГО АКТИВА, ВВЕДЕНИЕ МЕТОДА "ГАЛСТУК-БАБОЧКА".

ABSTRACT

Dissertation for Master’s degree: ___ p., __ fig., __ tables, __ sources.

The object of study is the process of general assessment of the cybersecurity risk by a functional method at enterprises of Ukraine.

The aim of the thesis is to improve the cybersecurity at Ukrainian enterprises through risk assessment by a functional method. Methods: comparison, analysis, modeling, assessment.

The special part describes the characteristic of a typical information activity object used for applying method of risk assessment. I analyze the models for choose the optimal information protection system and the regulatory framework of Ukraine that regulates the information security and cybersecurity spheres. The process and models for assessing cybersecurity risks have been studied. Recommendations on the choice of the method and its application in practice are suggested. In the economic part, I was cost of information resources of the enterprise, the capital and operating costs of the means of protection were calculated to reduce the risk of cybersecurity. The practical importance of the work consists applying the chosen method of risk assessment, as well as in developing a methodology for preventing cyber security risks. The scientific novelty of the work is to develop a methodology for preventing information security risks by applying functional method of a risk assessment.

Key words: RISK ANALYSIS, RISK ASSESSMENT METHODS, CYBER-SECURITY, INFORMATION SECURITY, RISK MANAGEMENT, PRICE OF INFORMATION ACTIVITY, IMPLEMENTATION OF THE METHOD "BOW-n-TIE".

ЗМІСТ

ВСТУП

Актуальність. В сучасному світі, що характеризується неосяжним розміром інформаційних ресурсів та даних, якими володіють та мають в своєму розпорядку сучасні організації та підприємства, все більше уваги приділяється проблемам забезпечення захисту інформації.

Для захисту від різних атак та спроб вторгнення порушників з метою попередження можливих загроз необхідний аналіз та реєстрування ризиків кібербезпеки, а також впровадження комплексу дій, що охоплюють науково-дослідні роботи в області захисту інформації в кіберпросторі.

Головне завдання забезпечення кібербезпеки все частіше вирішується внаслідок поліпшення процесу управління інформацією на базі реалізації різних підходів і методів, дотримання нормативних вимог і застосування організаційних заходів. Метою роботи є підвищення інформаційної безпеки на підприємствах України за допомогою оцінки ризиків.

Ризики кібербезпеки є невід'ємною частиною інформаційної діяльності, що можуть відбуватися в інформаційній, соціальній, технічній інфраструктурі держави, організації чи в інформаційно-комунікаційних мережах, впливаючи на стан державних інформаційних ресурсів і національну безпеку.

Об'єктом досліджень в роботі є процес оцінки та управління ризиками кібербезпеки на підприємствах України. Дослідженню процесів реагування, обробки, розслідування та аналізу ризиків кібербезпеки присвячено багато публікацій. На сьогоднішній день існує стандартизована міжнародна нормативно-правова база.

З провадження інформаційних технологій майже у всіх сферах життя людини, виникає проблема із захистом і стабільною роботою цих систем.

З кожним днем зловмисники вигадують нові способи заволодіння даними, це безперечно пов’язано з розвитком технічного прогресу та розробкою нових методів вторгнення в інформаційну систему.

З міжнародної статистики, ми можемо прослідкувати таку тенденцію, що з кожним роком збільшується кількість випадків, їх різноманітність і найголовніше прибуток зловмисників.

Те, що раніше вважалося неможливим, на сьогоднішній день стає реальністю. Це можуть бути програмні і технічні закладки, може бути персонал, який з однієї сторони через свою неуважність, з іншої з корисливих мотивів, передає інформацію зловмиснику. Купуючи нову техніку чи програмне забезпечення, не можна бути впевненим, що в неї не вбудован закладний пристрій.

Практична цінність полягає в розробці алгоритму для обрання методу оцінки ризику кібербезпеки, а також розробці методики прийняття рішення щодо оцінки ризику для підприємств України.

Для того, щоб побудувати систему менеджменту кібербезпеки, комплексну систему захисту інформації або інших систем безпеки, необхідно провести аналіз і оцінювання ризиків. Існуючі на сьогодні засоби оцінки ризиків в переважній кількості засновані на статистичних підходах. У більшості країн подібна статистика не ведеться, як на державному рівні, так і на рівні підприємств. Саме це обмежує можливості засобів оцінки, наприклад відсутність інформації для використання вхідних даних для оцінки ризику.

Забезпечувати отримання інформації на доказовій основі - це головне призначення загального оцінювання ризику, для того, щоб приймати обґрунтовані рішення, що саме робити з конкретними ризиками та як вибрати оптимальний варіант їх обробки.

Структуроване керування ризиком забезпечується політикою безпеки, впровадженими процедурами та організаційними заходами на всіх рівнях в організації. Організація повинна мати розроблену політику безпеки чи стратегію, для того, щоб в подальшому вирішувати, як та коли потрібно проводити загальну оцінку ризику.

Успішність загальної оцінки ризику залежить від результату обміна інформацією та консультації з зацікавленими сторонами, установлення оточення. Останнє дає змогу визначити основні параметри та критерії керування ризиком. Установлення оточення передбачає врахування параметрів, які пов'язані з внутрішніми та зовнішніми процесами організації, а також її минулого досвіду стосовно конкретних ризиків. Також під час установлювання оточення визначають і погоджують цілі оцінювання ризику, його критерії та програму оцінювання ризику. Установлення зовнішнього оточення передбачає ознайомлення з культурним, правовим, фінансовим та конкурентним середовищем, в якому функціонує організація, коли установлення внутрішнього оточення передбачає з'ясування цілей, а також запроваджених стратегій їх досягнення, інформаційних потоків, можливостей організації стосовно ресурсів і знань, політик і процесів, а також сприймання цінностей і культури.

Для встановлення оточення процесу керування ризиком необхідно визначити обсяг проекту, процесу та діяльності стосовно тривалості та місця впровадження. Також визначити зв'язки між конкретним проектом чи діяльністю та іншими проектами. Необхідно мати визначення критеріїв ризику та знати які методології використовуються для загального оцінювання ризику.

Визначення критеріїв ризику передбачає прийняття рішень щодо характеру можливих наслідків та способу їх вимірювання. При визначенні

критеріїв необхідно визначити за якими критеріями прийматимуться рішення щодо необхідності оброблення ризику та критерії, за якими будуть прийматися рішення щодо прийняття чи допустимості ризику.

Загальне оцінювання ризику дає змогу впроваджувати необхідні міри на рівні підрозділів, проектів, конкретних ризиків або на рівні організації в цілому. Після завершення загального оцінювання ризику провадять обробляння ризику, що передбачає прийняття одного чи декількох підходящих варіантів, які дають можливість зменшити ймовірність виникнення ризиків та їх вплив на систему.

Таким чином, метою дипломної роботи, що має практичне і наукове значення, є аналіз вже існуючих методів аналізу ризику кібербезпеки та їх адаптація і впровадження на підприємствах.

РОЗДІЛ 1
АНАЛІЗ ФУНКЦІОНАЛЬНИХ МЕТОДІВ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ

1.1 Проблеми забезпечення кібербезпеки України та їх рішення

На сьогодні очевидною є тенденція до посилення кіберскладової у системах державної безпеки провідних країн світу. Значні здобутки інших держав у цій сфері, які підсилюють ефект технологічної залежності, а відповідно і вразливості інформаційної інфраструктури, інформаційних ресурсів України, обумовлюють необхідність якнайшвидшого впорядкування вітчизняної політики кібербезпеки.

Аналізуючи сучасний стан забезпечення кібербезпеки в Україні, слід відзначити низку основних проблемних питань та напрямів їх вирішення. При цьому варто звернути увагу, що така ситуація характерна не тільки для України, але й інших країн світу, на міжнародному рівні також тривають дискусії з цих питань. Водночас не можна не вказати, яка робота здійснюється у цьому напрямі. Прийнято Стратегію національної безпеки України від 26 травня 2015 року [5], в якій представлено нове бачення кібербезпеки як окремої складової національної безпеки держави, визначено загрози кібербезпеці і безпеці інформаційних ресурсів, а також шляхи її забезпечення. Міністерством інформаційної політики України для обговорення представлено проект Концепції інформаційної безпеки України [4], в якій окремим видом загроз визначено загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору. Триває дискусія за

участю профільних відомств та наукових установ щодо визначення ключових термінів у сфері кібербезпеки.

Очевидним є відсутність єдиної загальнодержавної системи забезпечення кібербезпеки. Головною є проблема координації діяльності та розмежування відповідальності державних органів, які мають повноваження у сфері кібербезпеки. В Україні в системі забезпечення кібербезпеки держави задіяні ряд державних органів, серед яких Міністерство оборони України та його спеціальні підрозділи – зокрема Головне управління розвідки, Служба безпеки України, Служба зовнішньої розвідки, Державна служба спеціального зв'язку та захисту інформації, Міністерство внутрішніх справ України, кіберполіція, створена у складі Національної поліції України в 2015 році.

На думку фахівців, доцільним було б створення Національного центру протидії кіберзагрозам, який би виконував керівну й координуючу функцію у сфері забезпечення кібербезпеки. Багато критично важливих функцій держави залежать від бізнес-партнерів, враховуючи Інтернет-провайдерів і постачальників, аналітичних та науково-дослідних установ, інших постачальників послуг державним органам.

Незважаючи на ризики, така практика сприяє підвищенню ефективності заходів із забезпечення кібербезпеки, акумулюючи зусилля всіх зацікавлених сторін. Для України було б корисним проаналізувати кращі зразки передового досвіду інших держав у сфері інституційного забезпечення кібербезпеки й адаптувати їх відповідно до вітчизняної специфіки. Практика свідчить, що кадрове забезпечення відомств у системі забезпечення кібербезпеки України є недостатнім.

Вирішення цієї проблеми, на мою думку, полягає не стільки у збільшенні кількості навчальних закладів, які готують відповідних фахівців та розширенні спеціальностей, а в посиленні їх спроможності

підтримувати постійний контакт з практикою та швидко впроваджувати технологічні інновації у навчальний процес. Крім того, масштаби та якість наукових досліджень з питань кібербезпеки бажають бути кращими.

Водночас слід зазначити, що неможливість залучити висококваліфікованих фахівців до структур забезпечення кібербезпеки держави пов'язана також із браком матеріальних та нематеріальних стимулів для таких фахівців на державній (військовій) службі. Без сумніву в умовах формування глобального інформаційного простору та набуття кіберзлочинністю транснаціонального характеру запорукою успіху у протидії кіберзагрозам є розвиток міжнародної співпраці. Це включає розробку міжнародних норм і принципів дій у кіберпросторі, формування системи колективного стримування кіберзагроз, захист критичних елементів кіберінфраструктури держави, обмін передовим досвідом та спільне навчання фахівців. Україні, яка бере участь у заходах ООН, Ради Європи, НАТО, інших міжнародних і регіональних організацій з питань розвитку й безпеки кіберпростору, боротьби з кіберзлочинністю та кібертероризмом, варто зайняти більш активну позицію щодо представлення та захисту національних інтересів у сфері кібербезпеки.

Отже, серед ключових завдань щодо формування загальнодержавної системи забезпечення кібернетичної безпеки України доцільно виділити такі, як формування нормативно-правової бази кібербезпеки, зокрема законодавче закріплення визначень основних термінів у цій сфері, забезпечення координації діяльності та розмежування відповідальності державних органів, які мають повноваження з кібербезпеки (можливим є створення єдиного координаційного органу), посилення їх кадрового забезпечення, розвиток співпраці держави та приватного сектору, активізація участі України в міжнародному співробітництві з питань кібербезпеки.

1.2 Відміна інформаційної безпеки від кібербезпеки та аналіз ризиків

В сучасному світі поняття “безпека” відіграє чи не найголовнішу роль у всіх життєвих процесах: біологічних, політичних, економічних, соціальних, технічних, територіальних і ін. Тому дуже важливо не тільки коректно визначати це поняття і його похідні, а й правильно застосовувати їх за призначенням. Порівнюючи терміни «Кібербезпека» і «Інформаційна безпека» необхідно розуміти їх важливість, оскільки важливість цих понять в сучасному світі дуже велика. Визначення терміну «кібербезпека» взято з ISO / IEK 27032 2012 [6]: « кібербезпека — стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі». І визначення цього ж терміну в Законі України “Про основні засади забезпечення кібербезпеки України” [3] «Кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі”.

Під кіберпростором тут розуміється, середовище, яке надає можливості для здійснення комунікацій в результаті функціонування сумісних комунікативних систем з використанням мережі Інтернет.

Кіберпростір - простір, в якому здійснюється функціонування і взаємодія кібероб'ектов.

Кібербезпека об'єкта - властивість об'єкта, що характеризує його внутрішні можливості же не бути причиною утворення збитків для зовнішнього середовища або обмежувати його величину допустимими нормами. При цьому слід розуміти, що збиток кібероб'єкту наноситься в результаті спеціально організованих кібератак. Під кібератакою розуміється навмисні дії в кіберпросторі, які здійснюються за допомогою засобів програмних або апаратних засобів, або технологічного обладнання, що спрямовані на порушення конфіденційності та цілісності інформаційних ресурсів, отримання доступу до цих ресурсів, порушення безпеки та режиму роботи

Наприклад, отримання секретних відомостей з різних аспектів. За джерела організації кібератаки можна поділяти на дві групи: зовнішні, по відношенню до об'єкта кібератаки і внутрішні. Таким чином, джерелом внутрішньої кібератаки може бути персонал об'єкту кібератаки або персонал, який має доступ до його програмного забезпечення, якщо за діями цього персоналу немає належного контролю. Випадки зовнішніх кібератак описуються досить часто, особливо на мережі банків і фінансових організацій з метою привласнення грошей з чужих рахунків і карт приватних користувачів.

При використанні будь-якої комп’ютерної системи (КС) користувач, довіряя цій системі, покладається на безпеку її комп’ютерних компонентів, тобто на кібербезпеку КС. Задача полягає в тому, щоб оцінити можливі ризики через недостатню кібербезпеку КС. Назвемо ці ризики - ризиками довіри. Маємо ризики довіри, котрі існують для користувача, якщо він покладається на недостатньо надійну, недостатньо захищену і недостатньо безпечну для користувачів КС. Основною технологічною складовою будь-якої КС є автоматизована інформаційна система (АІС). Сучасні підходи до створення безпечних АІС припускають,

що для того, щоб на безпеку системи можна було покластися, повинні бути побудовані моделі загроз, моделі захисту, оцінені ризики порушення безпеки, вжиті заходи щодо забезпечення безпеки, придбані і впроваджені необхідні засоби забезпечення безпеки. При цьому на всіх етапах створення і експлуатації АІС існують системи вимог, які повинні виконуватися, для того щоб безпеки системи можна було б довіряти.

В сучасному світі група фахівців (або навіть одна людина) здатні за допомогою технічних і інформаційних засобів нанести непоправної шкоди військової, економічної, технологічної, політичної та інформаційної безпеки будь-якої держави. Тому більшість дій, здійснюваних сторонами в кібервійні, впливає на міждержавні відносини і може привести до політичного протистояння. Застосування Російскою Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на головне місце протиборства. РФ використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпал національної та релегійної ворожнечі, зміну конституційного ладу насильницьким шляхом чи порушення суверенітету та територіальної цілісності України.

Поняття «Інформаційна безпека держави» згідно Концепції інформаційної безпеки України [4] забезпечується шляхом захисту національного інформаційного простору від інформаційних загроз та через сприяння його сталому розвитку задля реалізації життєво важливих інтересів та потреб громадянина, суспільства і держави в інформаційній сфері.

Складність цього поняття полягає в тому, що сам предмет, безпеку якого визначається, не визначений як за внутрішньою структурою, так і за внутрішнім властивостями, які необхідні для формування вимог до його безпеки. Навіть саме визначення інформації, в наш час вельми

неоднозначно і суперечливо. Таким чином сформувати поняття безпеки такого предмета на підставі його внутрішньої структури і внутрішніх властивостей не уявляється можливим. Тим більше що до визначення інформаційної безпеки дано визначення зазначених в ньому складових: Конфіденційність інформації - такий стан інформації, при якому доступ до неї тільки у об'єктів з наявністю прав на неї. Порушення цілісності інформації - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст. Доступність інформації - це властивість інформаційного ресурсу, яка полягає в тому, що користувач, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки. До того ж, хочеться відзначити те, що обидва взятих для вивчення поняття фактично встановлюють еквівалентність термінів «безпека» та «захищеність».

Порівняйте самі, в першому терміні «безпека - захист» і в другому «безпека - стан захищеності». З іншої точки зору слід розрізняти два терміни: «Кібербезпека об'єкта» і «Кіберзахищеність об'єкта», що відповідає в англійській інтерпретації «Cyber safety object» і «Cyber security object». Перший термін визначений вище, другий термін, на мій погляд, повинен бути визначений таким чином: “Кіберзахищеність” об'єкта - властивість об'єкта, що характеризує його зовнішні можливості запобігати утворенню шкоди від кібератак або обмежувати його величину допустимими нормами. Що стосується терміну «інформаційна безпека», то має сенс поки міркувати тільки про захищеність інформації. Тому термін «безпека інформації», на даний момент часу визначається тільки намірами її володаря і нічим другім. Це дає підстави стверджувати, що термін «інформаційна безпека» на даний момент часу (поки не визначено коректно, що таке інформація і яка її внутрішня структура та властивості) не коректне по своїй суті. Замість нього можна запропонувати термін

«інформаційна захищеність» і використовувати для нього визначення викладене раніше тобто : «Інформаційна захищеність - захист конфіденційності, цілісності та доступності інформації», що, на мій погляд, відповідає реальному стану розглянутої проблеми.

1.3 Функціональні методи оцінки ризиків

Для того щоб відповідальним сторонам краще зрозуміти ризики, які впливають на результативність запроваджених засобів контролю та досягнення поставлених цілей, необхідне загальне оцінювання ризику. Саме це дає основу для прийняття рішень для найбільш відповідного підходу оброблення ризиків. Вихідні дані загального оцінювання ризику - це вхідні дані для процесів прийняття рішень в організації.

Процес який дає змогу ідентифікувати, аналізувати та оцінювати ризик називається - загальним оцінюванням ризику, що показано на рисунку 1.

Спосіб реалізації цього процесу залежить від багатьох факторів, таких як оточення керування ризиком, методів та методик, які використовують для загального оцінювання ризику.

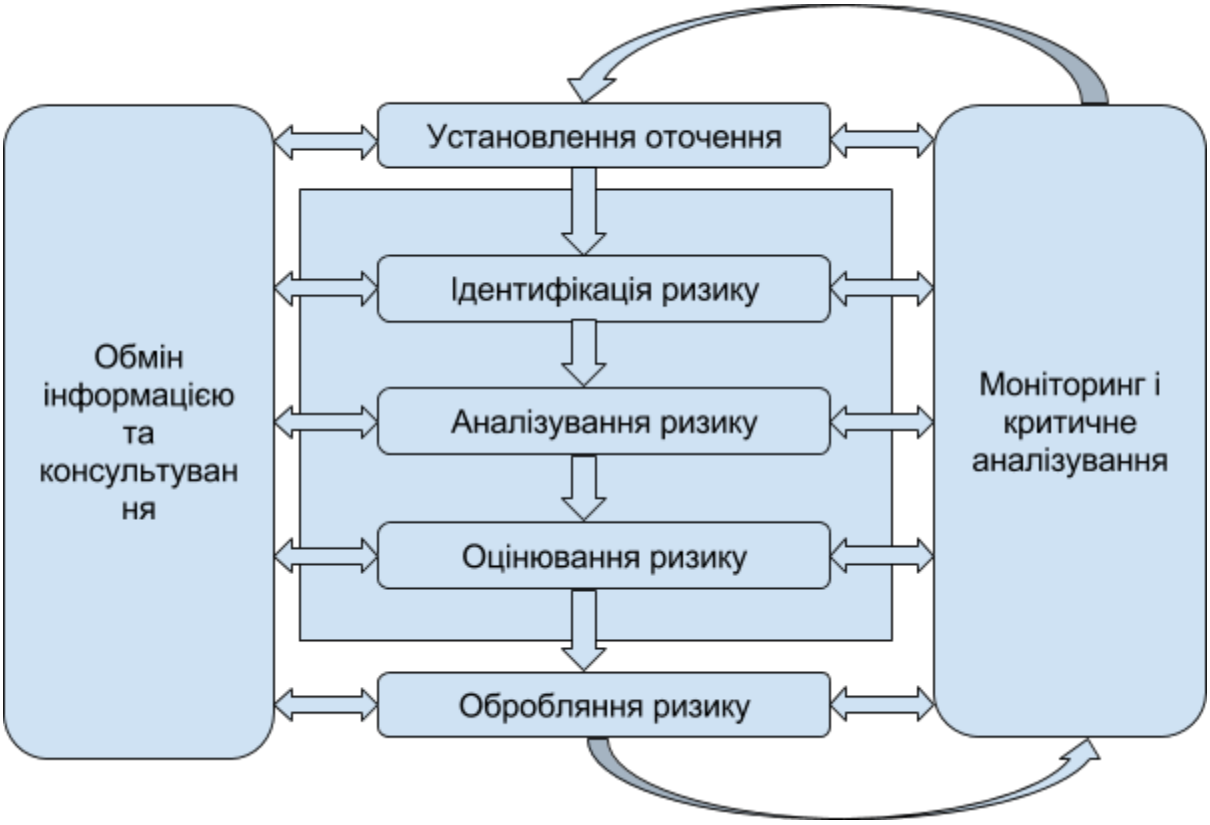

Рисунок 1.1 Процес загального оцінювання ризику

Процес виявлення, усвідомлення та реєстрування ризику називається - ідентифікуванням ризику, його призначення - визначити, які саме ситуації можуть виникнути, що можуть впливати на досягнення поставлених цілей організації. Після того, як ризик ідентифіковано, організація має визначити будь-які наявні засоби контролю, стосовно конструктивних особливостей, персоналу, процесів і систем.

Які існують методи ідентифікування ризику:

- доказові методи, наприклад, застосування переліків контрольних запитань і критичне аналізування даних;
- системні методи групової роботи, коли група експертів систематично ідентифікує ризики за допомогою структурованого набору навідних фраз або запитань;
- та інші.

Можна використовувати допоміжні методи, для того щоб поліпшити точніть і повноту ідентифікування ризику. Наприклад “Мозкову атаку” чи “Метод Дельфі”. Особливу увагу під час ідентифікування ризику необхідно приділяти організаційним та людським чинникам, враховувати відхили від очікуваних станів, а також події, які пов’язані з технічними та програмними засобами. Поглиблене розуміння ризику дає змогу прийняти рішення щодо найбільш відповідних стратегій і методик обробляння ризику.

Аналізування ризику передбачає розглядання причин і джерел ризику, їхніх наслідків та ймовірностей виникнення цих наслідків. Для того щоб виміряти рівень ризику необхідне кількісне оцінювання потенційних наслідків, які виникають за настання певної ситуації чи обставин.

Методи, використовувані під час аналізу ризику, можуть бути якісними, напівкількісними чи кількісними. Якісне загальне оцінювання дає змогу позначити наслідок, імовірність і рівень ризику такими термінами щодо рівня значущості, як “високий”, “середній” та “низький”, поєднати наслідок та ймовірність і оцінити рівень ризику, який випливає з цього, відповідно до якісних критеріїв. Напівкількісні методи передбачають застосування числових шкал оцінювання наслідків і ймовірностей та їх поєднання, щоб отримати рівень ризику за деякою формулою. Кількісний аналіз дає змогу практично оцінити значення наслідків, а також обчислити значення рівня ризику в конкретних одиницях, визначених під час установлення оточення, але повне кількісне оцінювання не завжди може бути можливе через нестачу інформації про систему, даних та інших чинників.

Для визначення рівня ризику необхідно мати адекватні та результативні засоби контролю, та мати відповіді та такі запитання:

- які засоби контролю, пов’язані з конкретним ризиком, наявні?
- чи дають змогу ці засоби контролю адекватне оброблення ризику?
- чи функціонують на практиці засоби контролю так, як передбачено, і чи можна, за потреби, продемонструвати їхню результативність?

Оцінювання ризику грунтується на розумінні ризику, набутому під час аналізу ризику, і слугує для прийняття рішень щодо подальших дій.

Рішення мають бути щодо:

- потреби в оброблянні ризику;
- приоритетів оброблення;
- доцільності виконання якоїсь роботи;
- вибору з низки напрямів тих, яких треба дотримуватись.

Придатний метод оцінювання має бути доречним щодо ситуації, забезпечувати отримання результатів для обробляння у найкращій формі розуміння ризику, для того щоб ризик можна було відстежити, відтворити чи перевірити. Метод обирається зважаючи на цілі дослідження, потреби тих, хто приймає рішення, діапазон ризиків, що аналізуються та потенційну величину наслідків, а також на ступінь фахової компетентності та потреби в людський та інших ресурсах. Більш простий запроваджений метод, якщо від задовольняє вище вказані критерії, може давати кращі результати, ніж складна, але недостатньо повна процедура.

Також на вибір методу оцінювання ризику впливають компетентність, досвід та здібності групи оцінювання ризику, обмеження часу, наявний бюджет у разі, якщо будуть залучатися зовнішні ресурси. Від кількості наявної інформації про ризик, причини його виникнення та наслідки, залежить можливість визначення характеру ризику.

Усі методи загальної оцінки ризику класифікують різноманітними способами, щоб краще розуміти їх сильні та слабкі сторони. На кожному

етапі процесу оцінювання ризику методи застосовують їх початкову класифікацію.

1. ідентифікування ризику;
2. аналізування ризику - якісне, напівкількісне чи кількісне оцінювання ймовірності;
3. загальне оцінювання результативності будь-яких наявних засобів контролювання;
4. аналізування ризику- кількісне оцінювання ризику;
5. оцінювання збитків.

Для кожного етапу процесу загального оцінювання ризику застосування методу подано як “ЗАВЖДИ ЗАСТОСОВНИЙ” (ЗЗ), “ЗАСТОСОВНИЙ” (З) чи “НЕЗАСТОСОВНИЙ” (НЗ). Дані стосовно функціональних методів оцінки ризику наведені нище у таблиці для ознайомлення.

Таблиця 1.1 Застосовність функціональних методів аналізування для загального оцінювання ризику

Методи та засоби аналізування	**Процес загального оцінювання ризику**

	Ідентифікування ризику	Аналізування ризику			Оцінювання ризику
		Наслідок	Імовірність	Рівень ризику	
Дослідження небезпечних чинників і працездатності (HAZOP)	ЗЗ	ЗЗ	З	З	З
Аналізування небезпечних чинників і критичні точки контролю (HACCP)	ЗЗ	ЗЗ	НЗ	НЗ	ЗЗ
Аналізування за схемою “краватка-метелик”	НЗ	З	ЗЗ	ЗЗ	З
Технічне обслуговування, зорієнтоване на забезпечення безвідмовності	ЗЗ	ЗЗ	ЗЗ	ЗЗ	ЗЗ

Аналізування паразитних схем	З	НЗ	НЗ	НЗ	НЗ
Аналізування видів і наслідків відмов	ЗЗ	ЗЗ	ЗЗ	ЗЗ	ЗЗ
Аналізування рівнів захисту (LOPA)	З	ЗЗ	З	З	НЗ

Ознаки методів описано стосовно:

- складності проблеми і методів, потрібних для її аналізування;
- характеру та ступеня невизначеності загального оцінювання ризику з урахуванням обсягу наявної інформації й того, що потрібно для досягнення цілей;
- обсягу необхідних ресурсів з урахуванням часу та рівня фахової компетентності, потреб у даних або витрат;
- можливості методу щодо отримання кількісних вихідних даних.

У таблиці нище наведено приклади типів наявних методів загального оцінювання ризику і кожний метод класифіковано за цими ознаками як “ВИСОКИЙ”, “СЕРЕДНІЙ” або “НИЗЬКИЙ”.

Таблиця 1.2 Ознаки вибору функціональних методів оцінювання ризику

Тип методу загального оцінювання ризику	**Опис**	**Важливість чинників**	**Дає змог**

			у отримуватиі кількісніі вихіднідані

		Ресурси та можливості	**Характер і ступінь невизначеності**	**Складність**	
HACCP (Аналізування небезпечних чинників і критичні точки контролю)	Систематичний, метод забезпечування якості продукції, надійності та безпечності процесів за допомогою вимірювання та моніторингу перебування конкретних характеристик у визначених межах	Середня	Середня	Середня	Ні
LOPA (Аналізування рівнів захисту)	Дає змогу оцінювати засоби контролю та їх результативність	Середня	Середня	Середня	Ткк
Аналізування за схемою “краватка-метелик”	Простий схематичний спосіб опису й аналізування варіантів розвитку ризику, починаючи з небезпечних чинників та закінчуючи наслідками, з критичною перевіркою засобів контролю.	Середня	Висока	Середня	Так
FMEA & FMECA	FMEA (аналізування виду та наслідків відмов) - це метод, який дає змогу ідентифікувати характер відмов і чинники їх виникнення, а також їх впливи. Метод можна доповнювати аналізуванням критичності, за якого визначають важливість кожного виду відмов, застосовуючи якісний, напівкількісний чи кількісний підхід. Аналізування критичності може базуватися на ймовірності того, що характер відмови спричинить відмову системи, або на рівні ризику, асоційованому з	Середня	Середня	Середня	Так

	характером відмови, або на ступені пріоритетності ризику.				
Технічне обслуговування, зорієнтоване на забезпечення безвідмовності	Метод ідентифікування політик, які треба запроваджувати для керування відмовами так, щоб ефективно та результативно досягати необхідного рівня безпеки, готовності та економічності функціонування всіх типів устаткування	Середня	Середня	Середня	Так
Аналізування паразитних ефектів (аналізування паразитних схем)	Метод який дає змогу ідентифікувати помилки. Паразитний стан - це прихований стан технічного засобу, програмного засобу чи їх поєднання, який може спричинити виникнення небажаної події чи може перешкоджати виникненню бажаної події. Паразитні стани можуть спричиняти неправильне функціонування, зниження готовності систем, програмні затримки чи навіть смерть або травми персоналу.	Середня	Середня	Середня	Ні
HAZOP (дослідження небезпечних чинників працездатності)	Загальний процес ідентифікування ризику, щоб визначити можливі відхили від передбаченої чи очікуваної дії. Передбачає використання системи, яка базована на керувальних словах.	Середня	Висока	Висока	Ні

1.3.1 Метод HAZOP

HAZOP - це “дослідження небезпечних чинників і працездатності” (HAZard and OPerability study). Цей метод дає змогу ідентифікувати ризики для персоналу та устаткування організації. Це якісний метод, який базується на формуванні запитань, з допоміжними словами, для того, щоб визначити міру за якою завдання чи умови функціонування не можуть бути досягнені на кожному етапі проекту чи системи в цілому.

Зазвичай дослідження проводить група фахівців під час кількох засідань. Відмінність полягає в тому, що група розглядає небажані результати та відхили від очікуваних результатів і станів, а потім діє у звоторньому напрямі.

Метод HAZOP розроблено для аналізу систем хімічного виробництва, але його поширили на інші типи систем і складних процесів. До них належать, зокрема, механічні й електронні системи, процедури, системи програмного забезпечення.

Поточна інформація про систему або процедуру, що підлягають критичному аналізу слугує вхідними даними для дослідження методом HAZOP, а також ціль проекту та технічні характеристики проектованого об’єкта. Вхідними даними можуть бути: креслення, документи технічних вимог, технологічні карти, логічні діаграми і блок-схеми керування процесом, процедури функціонування й технічне обслуговування, а також процедури аварійного реагування. Наприклад, організаційні діаграми та посадові інструкції, проект контракту.

В процесі аналізу методом HAZOP розглядають проект і технічні умови (специфікації) досліджувальних процесу, процедури чи системи, аналізують кожну їхню частину, щоб виявити, які відхили від очукуваної поведінки можуть виникнути, і визначають потенційні причини та можливі наслідки певного відхилу. Під час аналізу використовують настановчі слова, загальновживані стосовно технічних систем. Аналогічні

слова, зокрема “надто рано”, “надто пізно”, “надто мало”, “надто довгий”, “надто короткий”, “неправильний напрямок” або “неправильний об’єкт”, “неправильна дія” можна використовувати для ідентифікування видів людських помилок.

Переваги використання методу HAZOP має такі переваги як застосування до широкого спектра систем та процесів, є засобом систематичного дослідження системи, передбачає формування групи людей, які мають досвід практичної роботи в цій сфері та дає змогу явно розглядати причини та наслідки людських помилок. Але також цей метод має певні обмеженості, такі як потреба у більшому періоді часу, більшої витрати коштів та вимагає більш високого рівня документування системи чи процесу.

1.3.2 Аналізування небезпечних чинників і критичні точки контролю (HACCP)

HACCP - аналіз небезпечних чинників і критичні точки контролю надає структуру для ідентифікування небезпечних чинників і запроваджування засобів контролювання на рівні всіх важливих частин процесу, щоб запобігати небезпечним чинникам і підтримувати якість, надійність і безпечність продукції.

Цей метод було розроблено, щоб гарантувати якість харчових продуктів у межах космічних програм NASA. Зараз HACCP застосовують організації, які виконують роботу у межах ланцюга виробництва та реалізації харчового продукту, щоб контролювати ризики, пов’язані з фізичними, хімічними чи біологічними забрудниками харчових продуктів.

Застосування HACCP починають з розглядання основної технологічної схеми чи схеми процесу, а також інформації про небезпечні

чинники, які можуть впливати на якість, безпечність або надійність продукції чи на результат процесу.

У плані методу HACCP визначають методики, яких треба дотримувати, щоб забезпечити контроль конкретних проекту, продукції, процесу чи процедури.

Цей метод має такі переваги як структурований процес, зосередженість на практичних аспектах того, як і на яких етапах процесу можна запобігати небезпечним чинникам і контролювати ризики, заохочує до контролювання ризиків протягом усього процесу, а не тільки інспекційного контролювання кінцевої продукції.

Обмеженості HACCP полягають у тому що він вимагає ідентифікувати небезпечні чинники, визначати ризики, притаманні цим чинникам, і розглядати їхню важливість як вхідні дані до процесу аналізування. Застосування заходів у разі, коли контрольні параметри виходять за визначені межі, може призвести до того, що не буде помічено поступових змін контрольних параметрів, які є статично значними і, відповідно, що до них треба застосувати належні дії.

1.3.3 Аналізування видів і наслідків відмов (FMEA) і аналізування видів, наслідків і критичності відмов (FMECA)

Метод аналізування видів і наслідків відмов використовується для визначення того, як складники, системи чи процеси можуть ставати непридатними до функціювання за проектною призначеністю.

FMEA дає змогу ідентифікувати усі потенційні види відмов різних частин системи, впливи, які ці відмови можуть чинити на систему, чинники виникнення відмов та способи уникнення відмов або зменшення їхніх впливів на систему. FMECA розширює FMEA, охоплюючи

ранжування кожного ідентифікованого виду відмови відповідно до його важливості чи критичності. Це аналізування критичності зазвичай якісне чи напівкількісне, але уможливлює також кількісне подання за використання даних щодо фактичної інтенсивності відмови.

Є кілька сфер застосування FMEA: FMEA проекту(чи продукції), яке застосовують стосовно складників і продукції, FMEA системи, яке застосовують стосовно систем, FMEA процесу, яке застосовують стосовно виробничих і складальних процесів, FMEA послуги і FMEA програмного забезпечення. FMEA і FMECA можна застосовувати під час проектування, виробляння чи функціювання технічної системи.

Для FMEA і FMECA потрібна досить докладна інформація про елементи системи. Інформація може охоплювати креслення чи блок-схему системи та її складників, основні відомості про функціонування кожного етапу процесу чи складника системи, докладні відомості про параметри середовища та інші параметри, хронологічні дані про відмови, зокрема дані щодо інтенсивності відмов, якщо вони наявні.

Переваги цього методу оцінки ризиків такі:

- широка придатність до видів відмов, пов’язаних з людиною, устаткуванням та системами, а також до технічних засобів, програмних засобів і процедур;
- змога ідентифікувати види відмов складників, їхні причини та наслідки для системи, а також подавати їх у зручному для сприйняття форматі;
- змога уникати затратних змін експлуатованого устаткування завдяки ідентифікуванню проблем на ранній стадії у процесі проектування;
- змога уникати затратних змін експлуатованого устаткування завдяки ідентифікуванню проблем на ранній стадії у процесі проектування;

Обмеженості:

- можливість використання лише ідентифікування окремих видів відмов, а не комбінацій видів відмов;
- для досліджень може бути потрібно багато часу та витрат, якщо їх належно не контролювати та не спрямовувати;
- дослідження можуть бути важкими та утомними в разу складних багатошарових систем.

1.3.4 Аналізування рівнів захисту (LOPA)

Метод LOPA - напівкількісний метод оцінювання ризиків, пов’язаний з небажаним подіюєю чи сценарієм. Він дає змогу проаналізувати, чи є достатніми заходи контролюи чи пом’якшування ризику.

Процес заснований на виборі парі причина-наслідок та ідентифікації рівня захисту, який запобігає впливу, що призводить до небажаного наслідку. Обчислюють порядок величини, щоб визначити адекватність захисту для зменшення ризику до прийнятного рівня.

LOPA - це основа для специфікування незалежних рівнів захисту (IPL) і рівнів цілісності безпеки (SIL) для контрольно-вимірювальних вистем, визначання вимог до рівнів цілісності безпеки (SIL) для контрольно-вимірювальних систем безпеки.

LOPA можна застосовувати, для сприяння результативному розподіленню ресурсів зменшення ризику, аналізуючи зменшення ризику, забезпечуване кожним рівнем захисту. Незалежні рівні захисту - система

пристоїв або дія, які спроможні запобігати тому, щоб сценарій призводив до свого небажаного наслідку, незалежно від причинної події чи будь-якого іншого рівня захисту, пов’язаних з цим сценарієм.

LOPA - одна з методик, використовуваних для загального оцінювання рівні цілісності безпеки у разі розглядання систем, пов’язаних з безпекою. Переваги методу полягають в можливості ідентифікувати найкритичніші рівні захисту та зусередженню ресурсів на них, дає змогу ідентифікувати операції, системи та процеси, захист яких є недостатнім, акцентує увагу на найважчих наслідках та потребує менше часу та ресурсів. Але цей метод також має свої мінуси. Вони полягають в тому, що метод LOPA зосереджує увагу одночасно на одній парі причина-наслідок і одному сценарії. Кількісні ризики можуть не враховувати відмови загального характеру.

1.3.5 Аналізування діаграми “краватка-метелик”

Для відображення ризику та зазначені низки можливих причин та наслідків використовують аналіз методом “краватка-метелик”. Його використовують коли ситуація не настільки складна, для повного аналізу дерева відмов, коли зусереджують увагу на забезпеченні впевненості у наявності бар’єру чи засобу контролю для кожного шляху відмов. Цей аналіз корисний, коли є чіткі та незалежні шляхи, що ведуть до відмови. Вихідні дані - проста діаграми, що показує основні шляхи ризику та запроваджені бар’єри для запобігання небажаним наслідкам або їх пом’якшування чи стимулювання бажаних наслідків або спричинення їм.

Аналізування діаграмою “краватка-метелик” має такі переваги - є простим для розуміння, уможливлює чітке графічне зображення проблеми, воно зосереджує увагу на засобах контролю, які запроваджено для запобігання та пом’якшення ризику, а також на їхній результативності.

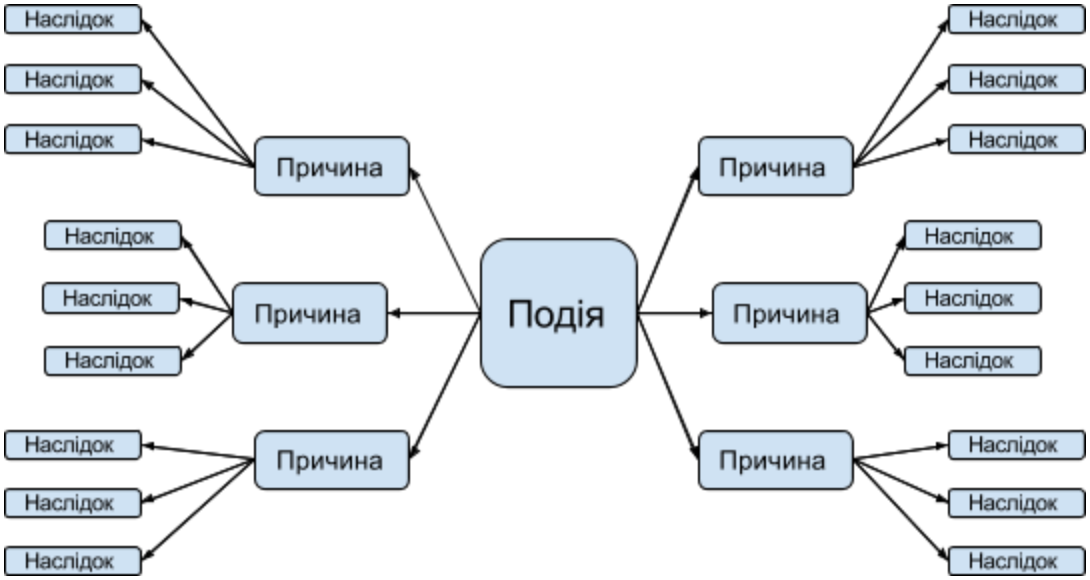

Рисунок 1.2 Приклад діаграми “краватка-метелик”

Метод можна застосовувати для аналізу бажаних наслідків. Для застосування методу не потрібен високий рівень фахової компетентності.

Але також метод має свої обмеженості. Він не дає змоги зобразити випадки одночасного впливу кількох причин на виникнення наслідків, також може надмірно спрощувати складні ситуації, особливо в разі кількісного подання.

1.3.6 Технічне обслуговування, зорієнтоване на забезпечення безвідмовності

Технічне обслуговування, зорієнтоване на забезпечення безвідмовності — метод визначення політики щодо керування відмовами,

яку має бути запроваджено так, щоб ефективно та результативно досягати необхідного рівня безпеки, готовності та економічності функціювання всіх типів устаткування. Рішення стосовно необхідності виконання певного завдання на технічне обслуговування чи внесення функціональних змін - є кінцевим результатом цього процесу.

Метод технічного обслуговування, зорієнтованого на забезпечення безвідмовності використовують, для забезпечення впевненості у виконанні належного результативного технічного обслуговування. Його зазвичай застостосовують на стадії проектування та розробки і потім запроваджують на стадії функціонування та технічного обслуговування.

Ідентифікування ризику зосереджено на ситуаціях, у яких може бути усунено потенційно можливі відмови чи зменшено їхню частоту чи наслідки в процесі виконання завдань технічного обслуговування. Увесь процес технічного обслуговування, зорієнтованого на забезпечення безвідмовності докладно задокументовують для подальшого користування та критичного аналізування.

1.3.7 Аналізування паразитних впливів (SA) і аналізування паразитних схем (SCA)

Метод аналізування паразитних впливів (SA) — заснован на можливості ідентифікувати помилки проектування. Паразитний стан — прихований стан технічного, програмного засобу чи їх поєднання, який може спричиняти небажану подію або стримувати виникнення бажаної події і який не зумовлено відмовою складника.

Аналізування паразитних схем (SCA) було розроблено наприкінці 1960-х років для NASA, для можливості забезпечувати перевірку цілісності проектів NASA. Воно було корисним інструментом для

виявлення ненавмисних контурів електричних кіл, а також сприяло виробленню рішень щодо відокремлення кожної функції. Паразитна схема — неочікуваний контур або логічний потік у системі, які за певних умов можуть ініціювати небажану функцію чи подавляти бажану функцію. Контур може охоплювати технічні засоби, програмні засоби, дії оператора чи комбінації цих елементів. Паразитні схеми не є результатом відмови технічних засобів. Йдеться про приховані стани, ненавмисно запроектовані в системі, закодовані в комп'ютерній програмі чи зумовлені помилкою людини. Вони поділяються на чотири категорії:

- Паразитні канали: неочікувані канали, якими струм, енергія чи логічна послідовність проходять у непередбаченому напрямку;

- Паразитна синхронізація: події, що відбуваються в неочікуваній або несумісній послідовності;

- Паразитні індикації: двозначні чи хибні відображення режиму функціювання системи, які можуть спричинити небажану дію системи чи оператора;

- Паразитні мітки: некоректне чи нечітке позначення функцій системи (наприклад, виводів, органів керування, шин дисплея), які можуть бути причиною введення оператором невірних настановних команд до системи.

Перевагами цього методу э ідентифікування помилок проектування, найкращі результати забезпечує його застосування з методом HAZOP, це є чудовим засобом розглядання системи, які мають кілька станів (наприклад об'єкти з безперервним або напівбезперервним характером виробництва).

Обмеження можуть бути такі як те, що процес дещо різниться залежно від того, чи застосовують його до електричних кіл, технологічного устаткування, механічного устаткування або програмних

засобів. Також метод залежить від правильності побудови деревоподібних мереж.

1.4 Постановка задачі дослідження

При загальній оцінці ризиків та застосуванні мір попередження виникнення загроз, необхідно визначити вартість реалізації заходів оцінки ризиків та засобів захисту (ціна пристроїв, витрати на обслуговування техніки, заробітна плата персоналу, витрати на комунальні послуги та інші).

Імовірні втрати від порушення кібербезпеки та ІБ відповідають кількісному значенню ризику, визначення якого є складною задачею. Існує значна кількість різних методик та методів кількісної оцінки ризику, що робить задачу обрання тих з них, що найкраще відповідатимуть потребам українських підприємств.

Також необхідне порівняння відомих моделей, ефективність яких була підтвердження на практиці, і обрання моделі, найкраще адаптованої до українських умов. Крім того, методи оцінки ризику відрізняються для різних сфер діяльності підприємств, а також мають відповідати нормативно-правовій базі України, що вимагає її аналізу.

За наявності параметрів можна розробити модель для прийняття рішень із оцінки ризику кібербезпеки із застосуванням найбільш придатного методу оцінки ризику кібербезпеки «краватка-метелик», яка б враховувала особливості діяльності та можливості прояву ризику.

1.5 Висновки до розділу 1

Розробка ефективної системи управління кібербезпекою стає

необхідною умовою для сучасного життя та ведення бізнесу. При цьому особлива увага надається процесу управлінню та оцінці ризиків, оскільки саме ці результати є необхідною основою для прийняття рішень з кібербезпеки.

Загальна оцінка ризиків – ключовий процес управління ризиками, оскільки на цьому етапі обираються засоби контролю за ризиком і визначається план робіт з кібербезпеки. Розроблено багато різних моделей та методів для прийняття рішень з кібербезпеки, але усі вони не є універсальними і орієнтовані для різних потреб. Для досягнення мети роботи для оцінки ризиків кібербезпеки був обран метод, що дає змогу в більшому обсязі детектувати та оцінити можливі ризики, оптимальні співвідношення між витратами на впровадження методу оцінки ризиків , застосування засобу захисту і рівнем захищеності системи.

Переважна більшість існуючих методик з прийняття рішень щодо оцінки ризику пропонують використання трьох з чотирьох методів обробки, а саме зниження, збереження та уникнення. Тому постає задача розробки рекомендацій, які б давали змогу зменшення ризику інформаційної безпеки до мінімуму.

РОЗДІЛ 2
РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ МЕТОДУ ОЦІНКИ РИЗИКІВ

2.1 Аналіз нормативно-правової бази, що регулює сфери кібербезпеки, ІБ та управління ризиками

Метою дослідження є аналіз нормативно-правової бази України та розгляд основних документів, які регламентують політику інформаційної безпеки та кібербезпеки в організації. Згідно з НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» [7] – політикою інформаційної безпеки є набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [8] встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі, зокрема й документів, які стосуються політики інформаційної безпеки. Загалом, політика інформаційної безпеки, як правила обробки інформації, розробляється згідно з положеннями НД ТЗІ 1.1-002 [7] та рекомендаціями НД ТЗІ 1.4-001 [8]. Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять такі документи:

- Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV [9];

• Закони України «Про інформацію» [1], «Про основи національної безпеки України» [10] , «Про Державну службу спеціального зв'язку та захисту інформації України» [11], «Про телекомунікації» [12], «Про захист інформації в інформаційно-телекомунікаційних системах» [2], «Про доступ до публічної інформації» [13], «Про оборону України» [14], «Про засади внутрішньої і зовнішньої політики» [15], «Про об'єкти підвищеної небезпеки» [16];

• Укази Президента України, зокрема про Доктрину інформаційної безпеки [17], Стратегію національної безпеки України [5] та Воєнну доктрину України [18];

• окремі положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБОУ.

Також ключову роль у забезпеченні кібербезпеки відіграють:

1) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2], який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ-системах;

2) Стратегія розвитку інформаційного суспільства в Україні, у запропонованих змінах до якої наголошується на необхідності створення національної системи кібербезпеки;

3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України», яким має бути впроваджено низку термінів, пов'язаних із кібербезпекою.

Стосовно управління ризиками, як галузь стандартизації та засіб підвищення ефективності роботи підприємства, є найбільш актуальним напрямком діяльності. Ступінь зрілості процесів управління ризиками істотно впливає на ефективність і безперебійність функціонування організації. На основі напрацьованих методик в області управління

ризиками почали розроблятися стандарти. Стандарти управління ризиками - це результат спільної роботи декількох провідних організацій, що займаються питаннями ризик менеджменту в Великобританії - Інституту Ризик Менеджменту (IRM), Асоціації Ризик Менеджменту та страхування (AIRMIC). У розробку стандартів великий внесок внесли професійні організації, що займаються питаннями управління ризиками і проявляють інтерес до тематики ризик менеджменту.

Організацією були розробленні стандарти з управління ризиками, базуючись, на практиці інших організацій - International Standard Organization (далі ISO). З метою реалізації ефективного ризик-менеджменту групою по ризик-менеджменту Технічного керуючого бюро ISO був розроблений міжнародний стандарт ISO 31000: 2009 «Risk management. Principles and guidelines» [19]. ISO 31000: 2009 дозволяє інтегрувати процес менеджменту ризику в загальне управління, стратегію і планування, менеджмент, процеси звітності, політику, цінності і культуру. В Україні на його основі розроблено національний стандарт ДСТУ IEC / ISO 31000: 2009 “Управління ризиком. Принципи та настанови” [19] - містить принципи, структуру і процес управління ризиками. Може бути використаний будь-якою організацією незалежно від її розміру, виду діяльності або галузі. Одними з головних переваг застосування ISO 31000: 2009 є усвідомлений підхід організації до ідентифікації і впливу на ризики на всіх рівнях управління, що призводить до зниження тимчасових і фінансових втрат організації, а також створення ефективного механізму управління організацією та прийняття рішень на різних організаційних рівнях.

Інший стандарт, розроблений комітетом ISO - ISO / IEC 31010: 2009 «Менеджмент ризиків. Методи оцінки ризиків» [20] зосереджений на оцінці ризиків. Оцінка ризику допомагає особам, які приймають рішення

зрозуміти ризики, які можуть вплинути на досягнення цілей також добре як адекватне управління вже на місці. ISO / IEC 31010: 2009 фокусується на поняттях, процесах і виборі методу оцінки ризиків. Областю застосування стандарту ISO / IEC 31010 є: концепція оцінки ризиків; оцінка ризиків процесу; вибір методів оцінки ризиків.

Стандарт забезпечує основу для прийняття рішення про найбільш доцільний підході, і використовується для прийняття рішення для конкретних ризиків, а також вибору між різними варіантами. ICO 31010 [20] не може бути використаний в цілях сертифікації, але служить керівництвом для внутрішніх або зовнішніх програм аудиту. Стандарт розроблений на додаток до ISO 31000 [19] та містить рекомендації щодо вибору і застосування методів оцінки ризику. Оцінка ризиків є невід'ємною частиною управління ризиками, який передбачає структурований процес, який має на меті виявлення того, які цілі організації можуть бути порушені ризиками.

15 березня 2016 р. Президент України підписав Указ, згідно з яким ввів у дію рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» [21], разом з тим постановив затвердити «Стратегію кібербезпеки України». Відтак, Рада національної безпеки і оборони України вирішила створити Національний координаційний центр кібербезпеки (НКЦБ) як робочий орган РНБО. Указом Президента України «Про Національний координаційний центр кібербезпеки» [22], було введено в дію запропонований центр. Вважаємо за необхідне виокремити принципові завдання НКЦБ:

1) слідкувати за даними про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

2) здійснювати системні заходи, спрямовані на посилення спроможностей суб’єктів сектору безпеки та оборони у боротьбі із

кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом, кіберзлочинністю, та у забезпеченні кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури;

3) координувати розгортання підрозділів кібербезпеки Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних органів спеціального призначення та приведення їх у готовність до виконання завдань в умовах особливого періоду, в умовах воєнного, надзвичайного стану і під час виникнення кризових ситуацій, що загрожують національній безпеці України;

4) моніторити стан розроблення національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих зі стандартами ЄС та НАТО тощо.

2.2 Рекомендації щодо вибору функціонального методу оцінки ризиків кібербезпеки

Невід'ємною частиною процесу управління ризику є оцінка ризику кібербезпеки, і являє собою структурований процес, при якому виявляють способи досягнення поставлення цілей, проводять аналіз ймовірностей виникнення та наслідків небезпечних подій для прийняття необхідності оцінки та обробки ризику.

Від вибору методів оцінки ризику та сфери застосування процесу залежить спосіб реалізації самого процесу оцінки ризику. Стандарт ДСТУ IEC/ISO 31010:2013 "Керування ризиком. Методи загального оцінювання ризику" [20] є загальним для всіх областей ризику. В умовах невизначеності та можливості виникнення планових та непередбачуваних обставин, управління ризику допомагає в прийнятті рішень.

Стандарт визначає 31 метод аналізу ризиків, з яких і будуть обиратися оптимальні методи для аналізу ризиків інформаційної безпеки. Перерахуємо їх найменування: “Мозкова атака”, “Структуроване чи напівструктуроване опитування”, “Метод Делфі”, “Переліки контрольних запитань”, “Попереднє аналізування небезпечних чинників (PHA)”, “Дослідження небезпечних чинників і працездатності (HAZOP)”, “Аналізування небезпечних чинників і критичні точки контролю (HACCP), “Загальне оцінюванная екологічного ризику”, “Структурований метод "Що - якщо" (SWIFT)”, “Аналізування сценаріїв”, “Аналізування впливу на діяльність (BIA)”, “Аналізування першопричини (RCA)”, “Аналізування видів і наслідків відмов (FMEA)”, “Аналізування дерева відмов (FTA)”, “Аналізування дерева подій (ETA)”, “Аналізування причин і наслідків”, “Аналізування причинно-наслідкових зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Дерево рішень”, “Загальне оцінювання надійності людини (HRA)”, “Аналізування за схемою "краватка-метелик", “Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Аналізування паразитних схем (SA)”, “Марковське аналізування”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”, “Криві FN”, “Показники ризику”, “Матриця “наслідок-ймовірність”, “Аналізування витрат і вигод (CBA)”, “Багатокритерійне аналізування рішень (MCDA)”.

Завдання вибору методу можна розділити на вибір придатного методу відповідно до галузі інформаційної безпеки за допомогою оцінки та вибір оптимального методу оцінки ризику.

З вище перелічених методів такі не придатні для аналізу інформаційної безпеки: “Дослідження небезпечних чинників і працездатності (HAZOP)”, “Аналізування небезпечних чинників і критичні точки контролю (HACCP)”, “Загальне оцінюванная екологічного ризику”. Розглянуті

методи які стосуються кожного етапу оцінки ризиків. Для ідентифікації ризиків не підходять такі методи: “Аналізування першопричини (RCA)”, “Дерево рішень”, “Аналізування за схемою "краватка-метелик", “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”. Таким чином, вибір зменшується і тепер вибираємо з 23 методів.

Оптимальність методів розглядається показниками наступних властивостей:

- ресурсомісткість (необхідні ресурси: тимчасові, інформаційні та інші);
- характеру і ступеня невизначеності оцінки ризику, заснованої на доступній інформації і відповідностям цілям;
- складності проблеми і методів, необхідних для аналізу ризиків.

З таблиці А.2 Додатка А, стандарту ДСТУ IEC/ISO 31010:2013 [20] вибираємо найоптимальніші за наведеними властивостями: “Структуроване опитування”, “Мозковий штурм” та “Переліки контрольних запитань”. Таким чином, для етапу ідентифікації ризику ми вибрали три методи, які можна комбінувати або використовувати найкращий з них.

Такі методи як “Структуроване чи напівструктуроване опитування”, “Переліки контрольних запитань”, “Мозкова атака”, “Метод Делфі”, “Попереднє аналізування небезпечних чинників (PHA)”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса” не підходять для етапу аналізу ризику. Таким чином залишається 21 метод, найбільш оптимальні з них: “Структурований метод "Що - якщо", “Аналізування впливу на діяльність (BIA)”, “Аналізування першопричини (RCA)”, “Аналізування видів і наслідків відмов (FMEA)”, “Аналізування дерева подій (ETA)”, “Аналізування причинно-наслідкових

зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Загальне оцінювання надійності людини (HRA)”, Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Аналізування паразитних схем (SA)”, “Матриця “наслідок-ймовірність”.

Для порівняльної оцінки ризику не підходять такі методи: “Переліки контрольних запитань”, “Структуроване чи напівструктуроване опитування”, “Мозкова атака”, “Метод Делфі”, “Попереднє аналізування небезпечних чинників (PHA)”, “Аналізування дерева подій (ETA)”, “Аналізування причинно-наслідкових зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Аналізування паразитних схем (SA)”, “Марковске аналізування”. З 21 вибираємо оптимальні, грунтуючись також на можливості отримання кількісних вихідних даних: “Аналізування дерева відмов (FTA)”, “Аналізування причин і наслідків”, “Аналізування за схемою "краватка-метелик", “Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”. З обраних обираємо функціональні методи оцінки ризиків, та маємо “Аналізування за схемою "краватка-метелик". Це і є обраний метод, після відбору методів оцінки ризику інформаційної безпеки по кожному етапу загального процесу на базі стандарту ДСТУ IEC/ISO 31010:2013 [20].

Практичний досвід побудови моделі загроз інформаційній безпеці виявив, що запропонований підхід значно спрощує завдання застосування методів оцінки ризику для конкретних інформаційних систем і заданого рівня кібербезпеки.

Таблиця 2.1 Порівняльні характеристики функціональних методів оцінки ризиків кібербезпеки

Тип методу загального оцінювання ризику	**Переваги**	**Недоліки**

HACCP (Аналізування небезпечних чинників і критичні точки контролю)	- Відносна легкість у використанні. - Забезпечення швидкого розподілу ризиків по рівням значення.	- Матриця має бути розроблена д конкретних обставин. - Важко встановити необхід графіки. - Ризикі не можна об'єднувати. - Результати залежать від рів деталізації аналіза.
LOPA (Аналізування рівнів захисту)	6. Метод потребує найменшої витрати часу та ресурсів. 7. Допомогає ідентифікувати найбільш важливі рівні захисту 8. Метод спрямований на серьозні небажані наслідки.	- Розглядає тільки одну пар причина-наслідок. - Кількісна оцінка ризиків не завж може бути отримана для загальн видів відмов. - Не застосовний до складн сценарієв ситуацій.
Аналізування за схемою "краватка-метелик"	- Метод дозволяє наочне уявлення проблеми. - Зорієнтований на засоби управління, які зменшують ймовірність шкідливих подій. - Метод застосовний до сприятливих подій. - Застосування методу не потребує залучення кваліфікованих експертів.	- Метод не дозволяє відобража пари причин, які виникаю одночасно та визивають наслідок. - Метод не дає змогу в повном обсязі оцінити складну проблем бо вона представлена в біл простому вигляді.
FMEA & FMECA	- Метод дозволяє ідентифікувати види відмов, які пов'язані з помилками персоналу або в роботі обладнання. - Метод дозволяє ідентифікувати види відмов компонентів та їх причини. - Метод дозволяє уникнути дорогих модицікацій обладнання та встановити вимоги системи безпеки. - Дає можливість отримати вхідні дані для розробки програми моніторингу.	- Може використовуватись тіль для ідентифікування окрем відмов. - Без контролю дослідження можу бути трудозатратними коштувати багато. - Потребує багато часу для біл складних багаторівневих систем.
Аналізування паразитних ефектів (аналізування паразитних схем)	- Аналіз скритих ефектів дозволяє ідентифікувати помилки проектування. - При спільному використанні з	- Метод залежить від правильно побудови деревоподібних схем. - Процес аналіза може відрізнятися залежності від того,

	методом HAZOP дає найкращі результати.	застосовується він до електричн схем або до технічного обладнан
HAZOP (дослідження небезпечних чинників працездатності)	- Метод забезпечує систематичний та повний аналіз системи чи процесу. - Наймаються фахівці з досвідом роботи, які ймовірно, й будуть розробляти рекомендації щодо обробки ризику. - Метод допомогає у виборі рішення та способу обробки ризику. - Дозволяє точно ідентифікувати причини та наслідки помилок.	- Детальний аналіз може займа багато часу, тому може коштува чимало. - Метод потребує написанню велик кількості документації. - Обговорення може бу зусереджено на окремих проблем проекту, а не відноситися широких чи зовнішніх проблем. - Метод обмежен задачами проек та метою дослідження.

Проаналізувавши недоліки та переваги функціональних методів оцінки ризику, можна стверджувати, що для оцінки ризиків кібербезпеки найбільш підходящим є метод “краватка-метелик”, який дає змогу наявно оцінити можливі ризики та наслідки.

Нижче на малюнку 2.1 наведена схема процесу побудови діаграми “краватка-метелик”.

Рисунок 2.1 - Схема алгоритму методу “краватка-метелик”

В діаграмі “краватка-метелик” можуть бути застосовані деякі види кількісної оцінки, наприклад, коли шляхи незалежні та відома ймовірність конкретних наслідків або результатів. Однак, необхідно зауважити, що в багатьох ситуаціях шляхи та бар’єри залежні один від одного, їх засоби управління можуть бути зв’язані з обраним методом оцінки, а отже, ефективність управління є невизначеною. Кількісну оцінку для методу “краватка метелик” роблять за допомогою методів FTA & ETA.

2.3 Висновки до розділу 2

Кожному виду діяльності, проектування і розробки продукції відповідає свій життєвий цикл: від концепції і розробки до стадії повного завершення експлуатації (використання).

Оцінка ризику може бути застосована на всіх стадіях життєвого циклу. Зазвичай її багаторазово використовують з різними рівнями деталізації на кожній стадії життєвого циклу для прийняття рішень.

Для різних стадій життєвого циклу встановлені різні вимоги і застосовні різні методи оцінки ризику. Після вивчення критеріїв та сфери застосування методів було обрано найбільш підходящий, який відповідає необхідним умовам проведення. Саме метод “краватка-метелик” дає змогу ідентифікувати ризики, оцінити можливі наслідки та запровадити заходи щодо запобігання ризиків. Аналіз методом “краватка-метелик” значно простіший для розуміння, а тому може бути корисним для обміну інформацією для більш складних методів оцінки ризиків кібербезпеки.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ ОБРАНОГО МЕТОДУ ОЦІНКИ РИЗИКІВ

3.1. Характеристика типового об’єкта інформаційної діяльності

Застосовуватися обраний метод оцінки ризиків буде до приватного акціонерного товариства «Телесистеми України». Основним напрямом діяльності підприємства є надання послуг зв’язку, а саме:

- мобільний зв’язок;
- інтернет провайдер;
- продаж обладнання.

Графік роботи підприємства з понеділка по п’ятницю з восьмої тридцять годин ранку до шостої години після полудня. Вихідні дні субота та неділя. Штат співробітників підприємства складається з 28 осіб, до яких належать:

- директор підприємства – 1 особа;
- бухгалтер – 2 особи;
- юрист – 1 особа;
- секретар – 1 особа;
- керівники відділів – 4 особи;
- фахівці з розробки програмного забезпечення – 3 особи;
- фахівці з тестування програмного забезпечення – 2 особи;
- фахівці з забезпечення зв’язку - 10 осіб;
- системний адміністратор – 1 осіб;
- охоронець – 2 особи;
- прибиральник – 2 особи.

ПАТ «Телесистеми України» має локальну обчислювальну мережу, яка включає 32 одиниць обчислювальної техніки (28 комп'ютерів, 4 сервери), та має вихід в мережу Інтернет, автоматизована система (АС) відноситься до класу АС 3.

В комп'ютерній мережі підприємства використовується топологія «ієрархічна зірка». Її відмінністю від «зірки» є використання декількох центральних вузлів, ієрархічно з'єднаних між собою зв'язками типу «зірка».

Для зв'язку комп'ютерів локальної мережі використовується стек протоколів TCP/IP. Для зв'язку з віддаленими офісами партнерів та державних структур на контролері домену налаштований VPN-сервер.

На підприємстві діє система охоронно-пожежної сигналізації та організована система відеоспостереження.

Інформацію, що становить цінність для підприємства, вказано в таблиці нижче у таблиці 3.1.

Таблиця 3.1 – Інформаційні активи підприємства

Правовий режим	**Інформація**	**В якій формі**	**Де зберігається**	**Умовні позначення**
Відкрита інформація	Інформація про підприємство, кількість робітників, послуги та спосіб їх оплати	Електроний та паперовий носії	На сервері, у кабінеті секретаря	1.1
	Організаційно-статутна документація	Електроний та паперовий носії	На сервері, у кабінеті секретаря та юриста	1.2
	Ліцензії	Електроний та паперовий носії	На сервері, у кабінеті директора	1.3
	Рекламні проспекти, інформація про тарифи, інформація для оприлюднення	Електроний та паперовий носії	На сервері	1.4
Інформація з обмеженим доступом	Договори з партнерами	Електроний та паперовий носії	На сервері, у кабінеті директора	1.5
	Персональні дані працівників підприємства	Електроний та паперовий носії	На сервері, на ПК бухгалтерів, у сейфі секретаря	1.6
	База даних клієнтів	Електроний носій	На сервері	1.7
	Організаційно-розпорядна документація	Електроний та паперовий носії	На сервері, у сейфах директора та секретаря	1.8

	Бухгалтерська звітність	Електроний та паперовий носії	На сервері, на ПК бухгалтерів, у сейфі бухгалтерів	1.9
	Технічні завдання	Електроний та паперовий носії	На сервері, у сейфі керівників відділів	1.10
	Розроблені проекти, їх документація	Електроний носій	На ПК програмістів, курівників відділів, на сервері	1.11

У таблиці 3.2 наведено матрицю доступу працівників ПАТ «Телесистеми України» до інформації.

Таблиця 3.2 – Матриця доступу працівників до інформації, що циркулює в ІТС

Працівник		**Директор**	**Секретар**	**Бухгал-тери**	**Юрист**	**Керівники відділів**	**Програмісти, тестувальники**	**Сист. адмін-р**
Роль в ІТС		К	К	К	К	ЛА	ЛА	АМ
Віддалений доступ		Ні	Ні	Ні	Ні	Ні	Ні	Так
Інформація	І1	R,W,D	R	R	R	R	R	R
	І2	R,W,D	R	R	R	R	R	R
	І3	R,W,D	R	R	R	R	R	R
	І4	R,W,D	R	R	R	R	R	R
	І5	R,W,D	-	R	R,W*,D*	R	-	-
	І6	R	R,W,D	R	R	R	-	-
	І7	R	R,W,D	R,W,D	R	R	-	-
	І8	R,W,D	R,W*,D*	R	R,W*,D*	R,W*,D*	R	R
	І9	R	-	R,W, D	R	-	-	-
	І10	-	-	-	-	R,W,D	R	-
	І11	-	-	-	-	R,W,D	R	-

У таблиці використовуються позначення для ролі в ІТС: К – користувач, ЛА – локальний адміністратор, АМ – адміністратор мережі; для вид доступу: R (read) – читання, W (write) – запис, D (delete) – видалення, * – лише для документів, створених користувачем.

На підприємстві діє матрична (проектна) організаційна структура, що зображена на рисунку 3.3. Керівники відділів керують командою програмістів, тестувальників і фахівцями з забезпечення зв’язку, кількість і склад яких може варіюватися залежно від потреб відділу.

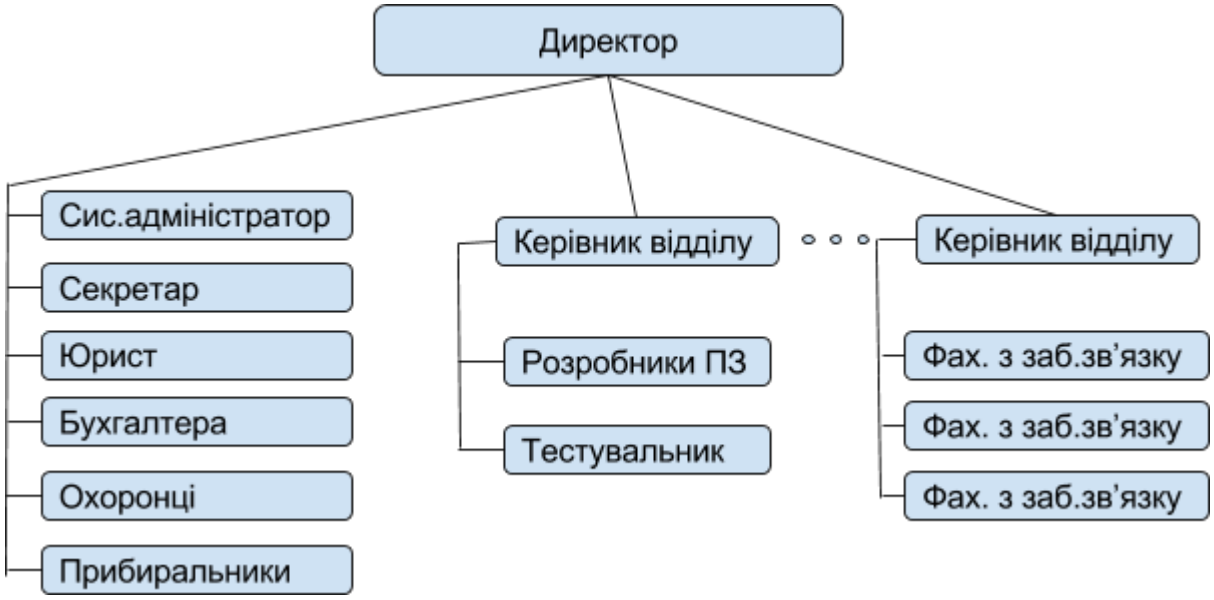

Рисунок 3.1 – Організаційна структура ПАТ «Телесистеми України»

Перелік апаратних та програмних забезпечень системи наведено в наступних таблицях.

Таблиця 3.3 – Список програмного забезпечення

Вид ПЗ	**Назва та версія ПЗ**	**Тип ліцензії, номер, дійсна до**	**Де встановлено**
Операційна система	9. Windows 10	10. Комерційна	PC1–PC28
	Windows Server 2008 R2	11. Комерційна	SR1–SR4
Прикладне	12. 7zip 16.04	13. GNU GPL	PC1–PC28

	14. AIMP v 4.50	15. FreeWare	PC1–PC28
	16. AppServ 8.6.0 (Apache 2.4.25, PHP 5.6.30, PHP 7.1.1, MySQL 5.7.17, phpMyAdmin 4.6.6)	17. GNU GPL	18. PC1–PC15, SR4
	Bacula 8.8	19. GNU GPL	PC1–PC28, SR1, SR4
	20. GIMP 2.8.22	21. GNU GPL	PC16 – PC28
	22. K-Lite Codec Pack 13.7.5	23. FreeWare	PC1–PC28
	24. LibreOffice 5.4.4	25. GNU GPL	PC1–PC28
	26. Skype 7.40.0.104	27. Adware	PC1–PC28
	28. STDU Viewer 1.6.375	29. FreeWare	PC1–PC28
	30. VirtualBox 5.1.30	31. GNU GPL 2	PC1–PC5
	32. WinDjView 2.1	33. GNU GPL	PC1–PC28
	34. Браузер Mozila Firefox 51	35. Mozilla Public License, GNU LGPL	PC1–PC28
	36. Браузери Opera 50, Google Chrome 63, Safari 5.1,Internet Explorer 10	37. Індивідуальні публічні 38. ліцензії	PC1–PC28
	Компілятори GCC6, Python 3.4.3, Ruby 2.2.3, Java Machine 8.60, Perl 5.22.0	39. GNU GPL	PC1-PC5
	Антивірус ESET NOD32 Antivirus Business Edition (3.0.695.0)	40. Комерційна, до 01.01.17	PC1–PC21, SR1, SR2
	DNS, cash-server, Active Directory, OpenSSH OpenSSl	41. -	SR3

Таблиця 3.4 – Характеристики ПК та серверів

Найменування	**Характеристики**	**Ум. позн.**
Комп’ютери програмістів, фахівців з тестування та керівників проектів (усього 9 ПК)	Intel B85/ Intel Core i5-4570 (3.2 ГГц)/ RAM 8 Gb / HDD 1Tb/ Intel HD Graphics/DVD±RW/ 500W	PC1–PC23

Комп’ютери директора, секретаря, бухгалтерів, юриста (усього 4 ПК)	Intel H81M-K/ Intel Pentium G3220 (3.0 ГГц)/ RAM 4 Gb/ HDD 500Gb / Intel HD Graphics/ DVD±RW/ 300W	PC24–PC28
Шлюз+ Firewall+VPN	MBD-X10SLL-F/Intel C222/ Intel Core i5-4570 (3.2 ГГц)/ RAM 8 Gb /HDD 320Gb/ 4xGigabit Ethernet/500W	SR1
Файловий сервер	MBD-X10SLL-F/Intel C222/ Intel Core i5-4570 (3.2 ГГц)/ RAM 8 Gb /HDD 1Tb/500W	SR2
Web-сервер	2 процесора Intel Xeon "Multi Core"/ чіпсет Intel i5000V, 2xPCI-E 8x, 2xPCI-X 64bit/133MHz/ 16 GB ECC DDR2 667 FBD (4/8 DIMMs)/ 800W Fiber blue	SR3 SR4

Таблиця 3.5 – Характеристики мереженого обладнання

Найменування	**Характеристика**	**Кіл-ть**	**Ум. позн.**
Комутатор CISCO SB SF100D-08 (SD208T-EU)	8-портовый Fast Ethernet настільний некерований комутатор	5	SW1-SW5
Комутатор Cisco SB SRW224G4-K9-EU	24-портовий Gigabit Ethernet настільний керований комутатор з доповненими 4 GE Combo mini-GBIC/SFP портами.	1	SW0

3.2 Розробка моделі порушника, моделі загроз та аналіз ризиків для ОІД

Згідно з нормативними документами: Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії та. ін. По відношенню до АС порушники можуть бути внутрішніми або зовнішніми.

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 АС, порушники поділяються на тих, хто має можливість 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 АС, впливу на базове програмне забезпечення системи і на склад і конфігурацію її устаткування (Р3).

За рівнем знань про АС усіх порушників можна класифікувати як таких, що мають невисокий рівень знань ІТ, володіють інформацією про функціональні особливості АС (Зн1), тих, що володіють середнім рівнем знань ІТ, мають досвід роботи з технічними засобами АС та їхнього обслуговування (Зн2), тих, що володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС (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 АС або недоліки проектування системи захисту інформації для реалізації спроб НСД (Сп3) та тих, хто використовує засоби активного впливу на АС, 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 ПАТ «Телесистеми України» порушників можна розділити на наступні групи (директор підприємства, як власник 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 – конкуренти.

ПЗ3 – кримінальні структури.

ПЗ4 – хакери.

ПЗ5 – технічний персонал з обслуговування будівлі та комунікацій.

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

Таблиця 3.6 – Модель порушника

Порушник	**Рівень знань ІТ**	**Рівень знань про ОІД**	**Місце дії**	**Час дії**	**Рівень можливостей**	**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
ПЗ5	Зн1, Зн2	-	М2	Ч1,Ч2	-	Сп3	Ц1	низький

Оцінка ризику ІБ ТОВ «ТелУкр»

Згідно з НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» пункту 4.4 [8]: Необхідно скласти перелік загроз, описати методи та способи їх реалізації, для створення моделі загроз. Цей перелік має бути максимально повним і розглянутий детально.

Для кожної з загроз необхідно визначити:

- які властивості інформації та системи вона порушує;
- причини та джерела виникнення;
- можливі способи здійснення загроз (вразливості, через які загроза реалізується).

Для формування моделі загроз я використовувала переліки загроз, які запропоновані у стандарті ISO/IEC 27005:2011 [25].

Для оцінки ризику високого рівня, щоб визначити ризики, рівень яких вище прийнятного, використовується матриця зумовлених значень, яка пропонується міжнародним стандартом ISO/IEC 27005:2011[25] наведена у таблиці 3.7. Для визначення ризику необхідно визначити цінність інформаційного активу, вірогідність загрози та рівень

вразливості.

Таблиця 3.7 – Матриця зумовлених значень

	Вірогідність виникнення загрози	**Низька (Н)**			**Середня (С)**			**Висока (В)**		
	Готовність вразливості	Н	С	В	Н	С	В	Н	С	В
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

При оцінці готовності вразливості, через яку може реалізуватися загроза, враховуються зручність (можливість) використання вразливості джерелом загроз, складність використання, необхідні кошти, можливість застосування неспеціалізованої апаратури.

Для ПАТ «Телесистеми України» прийнятним рівнем ризику було обрано 4. Результати оцінки ризику високого рівня наведено у таблиці 3.8.

Щоб передбачити усі можливі варіанти збитку, необхідно проаналізувати зв’язок між вразливістю, загрозою і впливом на актив.

Ризики інсайду – навмисного порушення безпеки співробітниками. Для цих ризиків можливе застосування лише одного методу обробки –

зниження. Так, для ПАТ «Телесистеми України» можна рекомендувати, у першу чергу, додати в штат посаду спеціаліста з інформаційної безпеки. Після цього необхідно проаналізувати ефективність застосування таких способів зниження ризику, як придбання DLP-системи (системи запобігання витоку даних), підвищення заробітної плати, підвищення культури підприємства та покращення умов праці. Особливу увагу варто приділити керівникам відділів, які мають доступ до повного коду проектів, та документації, а не частково.

3.3 Висновки до розділу 3

У даному розділі було проаналізовано ризики типового об’єкту інформаційної діяльності України та запропоновано заходи із управління ризиками, рівень яких перевищує прийнятний рівень. Для ризику втрати та компрометації цінних інформаційних ресурсів підприємства через кіберзагрози було розглянуто два методи управління ризиком: зниження ризику за допомогою допоміжних системи або найму спеціаліста з інформаційної безпеки та попередження ризику за допомогою попереднього аналізу ризику кібербезпеки. Було доведено, що економічна ефективність перенесення ризику значно перевищує відповідний показник для зниження.

РОЗДІЛ 4
ЕКОНОМІЧНА ЧАСТИНА

4.1 Вступ

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:

- вірогідні втрати від реалізації кіберзагроз;
- капітальні та експлуатаційні витрати для зниження ризику за допомогою засобів захисту;
- витрати на кібербезпеку при застосуванні методу оцінки ризиків;
- порівняти можливі витрати на запровадження необхідних мір та зменшення ризику з можливими втратами без запровадження методу оцінки ризиків кібербезпеки.

4.2 Впровадження заходів при використанні методу “краватка-метелик”

Система вимог щодо зменшення ризику повинна бути настільки сповнена, щоб її виконання дозволяло повністю охоплювати усі можливі істотними ризиками загрози. Тільки в цьому випадку можна буде міряти рівень довіри до безпеки використовуваної системи рівнем виконання вимог. Стосовно до проблем безпеки АІС прийнято використовувати термін - «інформаційна безпека». При виконанні системи вимог інформаційної безпеки (ІБ) 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 ІБ 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 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 формулюються 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.

4.3 Розрахунок поточних (експлуатаційних) витрат

Таблиця 4.1 – Характеристики та вартість мереженого обладнання

Найменування	**Характеристика**	**Кіл-ть, шт**	**Вартість, грн**	**Загальна вартість, грн**
Комутатор Cisco SB	24-портовий GigabitEthernet	4	5 000	20 000

SRW224G4-K9-EU	настільний керований комутатор з доповненими 4 GE Combomini-GBIC/SFP портами			
Загальна сума ($В_{мо}$)				20000

Таблиця 4.2 – Характеристики та вартість апаратних засобів

Найменування	**Характеристика**	**Кіл-ть, шт**	**Вартість**	**Загальна вартість, грн**
Сервери для моніторингу	Intel B85/ IntelCore i5-4570 (3.2 ГГц)/ RAM 16 Gb / HDD 1Tb/ Intel HD Graphics/DVD±RW/ 500W	5	14 000	70 000
Монітор Samsung C24F390F	Діагональ 24 " / 1920x1080 / 60 Гц	10	4 500	45 000
Комп'ютерна мишкаGeniusXscroll G5 USB Black	1000 dpi / оптична	10	150	1 500
Клавіатура Genius KB-110X USB Black	MBD-X10SLL-F/Intel C222/ IntelCore i5-4570 (3.2 ГГц)/ RAM 8 Gb /HDD 320Gb/ 4xGigabit Ethernet/500W	10	250	2 500
Загальна сума ($В_{аз}$)				119000

Таблиця 4.3 – Характеристики та вартість програмних засобів

Вид ПЗ	**Назва та версія ПЗ**	**Тип ліцензії, номер, дійсна до**	**Вартість, грн**
Операційна система	Windows 10 Pro	Комерційна	6 000
	Браузери Opera 38, GoogleChrome 51, Safari 5.1,Internet Explorer 8	Індивідуальні публічні ліцензії	-
	Антивірус ESET NOD32 AntivirusBusinessEdition (3.0.695.0)	Комерційна, до 01.01.19	1 200
Загальна сума, грн			7 200

Таблиця 4.4 – Характеристики та вартість систем резервного копіювання

Найменування	**Характеристики**	**Кіл-ть**	**Вартість**	**Загальна вартість, грн**
Storage (сервер резервного копіювання)	IntelXeon E5-2650 (6 ядер)/2.0 ГГцRam: 16 Гб/ LAN: 1 Гбіт/с (RJ-45) - 2 шт. HDD: Seagate 2x1Tb -SATA HotPlug/500W	1	20 000	20 000
Загальна сума ($В_{рк}$)				20 000

Обстеження підприємства проводитиме стороння організація,

$$В_о = 20\ 000 \text{ грн.};$$

Проектування системи захисту проводитиме стороння організація,

$$В_п = 15\ 000 \text{ грн.};$$

Вартість річної ліцензії системи захисту ($В_л$) HP ArcSight складає 100 000 грн.

Таблиця 4.5 – Програмні продукти HP ArcSight

№	Найменування
1	HP ArcSightLgr 30GB/d 200Dev SW E-LTU
2	P ArcSight CONAPP 50 Con SW E-LTU
3	HP ArcSight SC 5.14 Eng SW E-Media
4	RTS Charge

Налаштування системи захиту проводитиме стороння організація,

$$В_н = 20\ 000 \text{ грн.};$$

Підключення джерел подій до системи проводитиме стороння організація,

$$В_{пд} = 10\ 000 \text{ грн.};$$

Розробку правил кореляції для сценаріїв виявлення інцедентів проводитиме стороння організація,

$$В_{рпк} = 10\ 000 \text{ грн.};$$

Розробку регламенту реагування на інциденти кібербезпеки проводитиме стороння організація,

$$В_{рр}= 10\ 000 \text{ грн.};$$

Розробку інструкцій оператора/аналітика/користувача проводитиме стороння організація,

$$В_{рі}= 7\ 000 \text{ грн.};$$

$$В_{ТО} = 119\ 000 + 20\ 000 + 7\ 200 = 119\ 200 \text{ грн.}$$

$$В_{ТР} = 20\ 000 + 15\ 000 + 100\ 000 + 20\ 000 + 10\ 000 + 10\ 000 + 10\ 000 + 7\ 000 = 192\ 000 \text{ тис. грн.}$$

Для розрахунку машинного часу ми використаємо середню потужність серверу, яка складає 1,2 кВт і вартість електроенергії для приватних підприємств 1,67 грн.

$$З_{мч} = 1{,}2*1{,}67 = 2 \text{ грн.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p}$$

де Р – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{перв}$– первісна вартість ПК на початок року, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$– річний фонд робочого часу (система повинна працювати постійно, тому $F_р$= 8760 год).

$$C_{мч} = 1.2 \cdot 1 \cdot 1.67_e + \frac{15000 \cdot 0.25}{8760} + \frac{8200 \cdot 0.25}{8760} = 2.66$$

Вартість електроенергії, що споживається апаратурою протягом року ($C_е$), визначається за формулою:

$$C_е = C_{мч} \cdot F_р, \text{ грн},$$

$F_р$– річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки, складає 8760);

$$C_е = 2{,}66*8760 = 23\ 336 \text{ грн.}$$

Загалом вартість розгортання системи захисту кібербезпеки становитиме:

$$В_{сб} = 119\ 200 + 192\ 000 + 23\ 336 = 334\ 536 \text{ грн.}$$

Перекваліфікацією персоналу займатиметься сторонння організація.

Таблиця 4.6 – Вартість перекваліфікації персоналу

Минула посада	**Цільова посада**	**Вартість перекваліфікації**	**Необхідна кількість, осіб**	**Загальна вартість, грн**
Керівник відділу	Керівник системи	45 000	1	45 000
	Аналітик системи	35 000	1	35 000

Фахівець з забезпечення з’вязку	Фахівець з моніторингу та реагування	15 000	4	15 000
Загальна сума ($В_{мо}$)				95000

Загалом вартість розгортання системи захисту становитиме:

$$В_{сбп} = 334\ 536 + 95\ 000 = 429\ 536 \text{ грн.}$$

4.4 Розрахунок збитків на підприємстві за відсутності методу оцінки ризиків "краватка-метелик"

Визначення вартості інформаційних активів також може викликати складнощі. Активи можна розділити на матеріальні і нематеріальні. До матеріальних відносяться засоби обслуговування ІТС: апаратне забезпечення, мережеве обладнання (засоби передачі даних), запасні запчастини, документація і заробітна плата обслуговуючого персоналу. Вартісні характеристики цих активів зазвичай добре відомі або легко обчислюються.

Вартість нематеріальних активів має враховувати два види витрат: витрати на заміну або відновлення програмного забезпечення та даних, а також витрати при порушені цілісності, доступності та конфіденційності.

Якщо певні дані були втрачені, для їх відновлення будуть необхідні наступні засоби:

- якщо дані збереглися як інтелектуальний продукт (у вигляді думок, ідей, чернеток), то витратами буде оплата роботи операторів, що буде відновлювати дані на електронних носіях;

- якщо дані не збереглися ні у якому виді, то витратами буде оплата роботи групи спеціалістів з відновлення даних до етапу, на якому дані були втрачені, за умови, що актуальність даних не втрачена. Якщо збереглися певні матеріали або обладнання, що можна використати повторно, їх варто виключити із загальних витрат.

Для оцінки вартості конфіденційності активу необхідне дослідження додаткових умов:

42. якщо розголошення інформації ніяк не вплине на діяльність підприємства, то дані не мають вартості з цієї властивості;

43. якщо розголошення інформації, наприклад, конкурентам, означає крах усіх пов'язаних з нею бізнес-процесів підприємства, то вартість активу за цією властивістю може становити вартість повного відновлення або може бути рівна прибутку з бізнес-процесів;

44. якщо розголошення інформації частково вплине на бізнес-процеси, то і вартість за конфіденційністю становить частину від пункту 2.

Для оцінки вартості цілісності необхідно розрізняти помилки персоналу, помилки обладнання та зміни, внесені зловмисником. Також варто розрізняти дані за чутливістю до порушення цілісності:

- якщо зміна даних привела до прямих матеріальних втрат (неотриманий прибуток або зайві витрати) – це і є вартість активу за цілісністю. Але максимальні збитки можуть бути нанесені не завжди, оскільки будуть виявлені і відвернені, або компенсовані через повернення втрачених коштів.

- зміна даних також може викликати більші або менші втрати,

оцінити які може лише спеціаліст.

Порушення доступності доцільно розрізняти за часом. Якщо дані недоступні назавжди, ситуація аналогічна втраті цих даних. Часткову недоступність варто класифікувати за проміжками часу.

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_{п\ до}$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки до впровадження заходів, годин, даний показник складає приблизно $t_п = 4$ години;

$t_{п\ після}$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки після впровадження заходів, годин, даний показник складає приблизно $t_п = 1$ годину;

$t_{в\ до}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу до впровадження заходів, годин, даний показник складає $t_в = 4$ години;

$t_{в\ після}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу після впровадження заходів, годин, даний показник складає $t_в = 1$ годину;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі до впровадження заходів, годин $t_{ви}= 5$ годин;

$t_{ви}$ – час повторного введення загубленої інформації

співробітниками атакованого вузла або сегмента корпоративної мережі після впровадження заходів, годин $t_{ви}$= 1 годину;

$З_{о\ до}$ – місячна заробітна плата обслуговуючого персоналу (інженери ІБ) з нарахуванням єдиного соціального внеску, грн на місяць, складає 8000грн;

$З_{о\ після}$ – місячна заробітна плата обслуговуючого персоналу (фахівці з моніторингу та реагування) з нарахуванням єдиного соціального внеску, грн на місяць, складає 7 000грн;

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць, складає 15 000грн;

$Ч_{о\ до}$ – чисельність обслуговуючого персоналу (керівники відділів), осіб,

$Ч_{о\ після}$ = 4 осіб;

$Ч_{о\ після}$ – чисельність обслуговуючого персоналу (фахівці з забезпечення зв’язку), осіб,

$Ч_{о\ після}$ = 10 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб, $Ч_с$ = 14 осіб;

За вузол вважаємо команду розробників та тестувальників ПО, яка складається з 14 чоловік.

О – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі, складає 1 200 000 грн.;

І – число атакованих вузлів або сегментів корпоративної мережі;

$$I=5$$

N – середнє число можливих атак на рік.

N=10

Втрачена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_{п\_до} = \frac{\sum З_с * Ч_с}{F} \cdot t_п$$

До впровадження заходів:

Після впровадження:

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$– витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \cdot t_{ви}$$

До впровадження заходів:

Після впровадження заходів:

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в$$

До впровадження заходів:

Після впровадження заходів:

Втрати від простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньо-годинного прибутку і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_c} \cdot (t_n + t_в + t_{ви})$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день)

До впровадження заходів :

$$U_{до} = 5250+6562.5+8128=19\ 937.5 \text{ грн.}$$

Після впровадження заходів:

$$U_{після} = 1312.5+1312.5+1875=4550 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum\sum U \cdot N \cdot I$$

До впровадження заходів:

$$В_{до}=19\ 937.5*10*5=996\ 875\ грн.$$

Після впровадження заходів:

$$В_{після} = 4\ 500*10*5 = 67\ 500\ грн.$$

Різницю від втрат до впровадження заходів на установі та після вирахуємо по формулі:

$$\Delta В = В_{до} - В_{після}$$

$$\Delta В = 996\ 875 – 67\ 000 = 929\ 375\ грн.$$

Вирахуємо термін протягом якого окупиться впровадження центру оперативного управління кібербезпекою за формулою:

$$T = \frac{Bsoc}{\Delta B}$$

4.5 Висновки до розділу 4

Існує група ризиків кібербезпеки, зменшення яких за допомогою засобів захисту неможливе через надмірну вартість. У даному розділі було розраховано капітальні та експлуатаційні витрати на засоби захисту для зменшення ризику, рівень якого вище прийнятного. Загалом вартість розгортання системи захисту становитиме:

$$В_{сбп} = 334\ 536 + 95\ 000 = 429\ 536\ грн.$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum \sum U \cdot N \cdot I$$

$B_{до}$=19 937.5*10*5=996 875 грн.

Після впровадження заходів:

$B_{після}$ = 4 500*10*5 = 67 500 грн.

Різницю від втрат до впровадження заходів на установі та після вирахуємо по формулі:

$$\Delta B = B_{до} - B_{після}$$

$$\Delta B = 996\ 875 – 67\ 000 = 929\ 375 \text{ грн.}$$

ВИСНОВКИ

У дипломній роботі було розроблено методику щодо запровадження системи захисту на основі аналізу ризиків кібербезпеки на типовому об’єкті інформаційної діяльності. В ході виконання поставлених в дипломній роботі задач були отримані наступні наукові та практичні результати:

- Було порівняно функціональні методи оцінки ризиків, що знаходить оптимальне співвідношення між витратами на засоби захисту і рівнем захищеності системи.
- Було зроблено детальний опис алгоритму аналізу ризиків кібербезпеки.
- Була проаналізована нормативно-правова база, що регулює управління ризиками та сферу інформаційної безпеки та зроблені висновки щодо її недоліків, що не дозволяє регулювання сфери страхування ризиків кібербезпеки.
- Були порівняні групи методів оцінки ризику ІБ і виявлено істотні обмеження у застосуванні відомих методів кількісної оцінки.
- Було проаналізовано ризики типового ОІД України та запропоновано заходи із управління ризиками, рівень яких перевищує прийнятний рівень. Було доведено, що економічна ефективність перенесення ризику значно перевищує відповідний показник для зниження.
- В економічній частині було розраховано вартість інформаційних ресурсів підприємства, капітальні та експлуатаційні витрати на засоби захисту для зменшення ризику.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про інформацію [Електронний ресурс]: Закон України від 02.10.1992, ред. 21.05.15 №2657-12. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12;
2. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: Закон України від 05.07.1994, ред. 19.04.14 № 80/94-вр. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-вр;
3. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: Закон України від 19.06.2015, ред. 05.10.17 №2163-19. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80;
4. Концепція інформаційної безпеки України [Електронний ресурс]: Проект від 09.06.2015. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf;
5. Стратегія національної безпеки України [Електронний ресурс]: Указ Президента України від 26.05.2015 №287/2015. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015;
6. Міжнародний стандарт ISO/IEC 27032:2012 « Информационные технологи. Руководящие указания по кибербезопасности» [Електронний ресурс]. – Режим доступу: https://www.iso.org/ru/standard/44375.html;
7. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс]: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340;

8. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [Електронний ресурс]: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341;
9. Конвенція Ради Європи про кіберзлочинність [Електронний ресурс]: від 07.09.2005 №994-575. Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_575;
10. Про основи національної безпеки України [Електронний ресурс]: Закон України від 30.11.2017 №964-15. – Режим доступу: http://zakon.rada.gov.ua/go/694-15;
11. Про Державну службу спеціального зв'язку та захисту інформації України [Електронний ресурс]: Закон України від 11.05.2007, ред. 09.12.2015 №3475-15. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/3475-15;
12. Про телекомунікації [Електронний ресурс]: Закон України від 02.10.1992, ред. 21.05.15 №2657-12. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1280-15;
13. Про доступ до публічної інформації [Електронний ресурс]: Закон України від 13.05.2011, ред. 01.05.15 №2939-17. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2939-17;
14. Про оборону України [Електронний ресурс]: Закон України від 06.12.1991, ред. 28.07.2016 №1932-12. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1932-12;
15. Про засади внутрішньої і зовнішньої політики [Електронний ресурс]: Закон України від 23.01.2008, ред. 30.11.17 №2411-17. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2411-17;
16. Про об'єкти підвищеної небезпеки [Електронний ресурс]: Закон України від 18.01.2001, ред. 26.04.14 №2245-14. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2245-14;

17. Про Доктрину інформаційної безпеки [Електронний ресурс]: Закон України від 25.02.2017, №47/2017. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/47/2017;
18. Воєнну доктрину України [Електронний ресурс]: Указ Президента України від 15.06.2004, ред. 02.09.15 №648. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/648/2004;
19. Международний стандарт ISO 31000: 2009 «Риск менеджмент. Принципы и руководства» [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/43170.html;
20. Міжнародний стандарт IEC 31010:2009 «Керування ризиком. Методи загального оцінювання ризику» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=51073.
21. Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" [Електроний ресурс]. – Указ Президента від 27 січня 2016 року http://zakon2.rada.gov.ua/laws/show/96/2016/paran11#n11;
22. Про Національний координаційний центр кібербезпеки [Електроний ресурс]. Указ Президента України від 07.06.2016 №242/2016 – Режим доступу: http://zakon2.rada.gov.ua/laws/show/242/2016 ;
23. Міжнародний стандарт ISO/IEC 27000:2014 «Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Визначення та загальні відомості» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=63411;
24. Домарев В. В. Безопасность информационных технологий. Системный подход. Киев.: ДиаСофт, 2010.;

25. Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742;
26. Рекомендації Національного інституту стандартів та технологій США «Risk Management Guide for Information Technology Systems», 2002 р. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf;
27. Сидоренко О. П. Управління ризиками для підприємців: Електронний курс eNano, 2014 р. / [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/studies/courses/4456/715/info;
28. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 2010. - 320 с.;
29. Арьков П.А. Разработка комплекса моделей для выбора оптимальной системы защиты информации в информационной системе организации: дис. к.т.н.: апрель 2009 / Павел Алексеевич Арьков; Волгоградский государственный университет. – Волгоград, 2009. – 410 с.;
30. Астахов А.М. Искусство управления информационными рисками / Астахов А.М. – М.: ДМК Пресс,. 2010. – 312 с.;
31. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. ? М.: Книжный мир, 2009. -352 с.;
32. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07. № 537-V // Відомості Верховної Ради України. – 2007. – № 12.– Ст. 102;

33. Перелік послуг з аутсорсингу у сфері інформаційної безпеки компанії IBM. [Електронний ресурс]. – Режим доступу: http://www-03.ibm.com/security/services/managed-security-services/;
34. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов.-М.: Горячая линия-Телеком. -2008.- 280 с.;
35. Гребенюк А. Аутсорсинг ИБ – краткий обзор рынка, 2014 р. [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/analytics/Market_Analysis/Outsourcing_Information_Security_overview_of_the_market;
36. Цуканова О.А., Смирнов С.Б. Экономика защиты информации: Учебное пособие. – СПб.: СПб ГУИТМО, 2007. – 59 с.;
37. Офіційний сайт Державної служби спеціальних телекомунікаційних систем і захисту інфор-мації. Електронний ресурс: «Біла книга Держспецзв'язку». — http://www.dstszi.gov.ua/dstszi/ — 47 с;
38. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Затв. постановою КМУ від 16.11.2002 р. №1772. Із змінами, внесеними згідно з Постановою КМУ від 08.12.2006 р. №1700. — 2 с.;
39. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. - 544 с.;
40. Міжнародний стандарт ISO/IEC 27037:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо ідентифікації, збору, придбання і збереження цифрових даних» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=44381;

41. Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств – участников Содружества Независимых Государств в сфере информатизации [Електронний ресурс]: документ 997_842 від 24.12.1999 – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=997_842;
42. Конституція України [Електронний ресурс]: документ №254к/96-вр від 28.06.1996, ред. 15.03.16. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/254к/96-вр/;
43. Инструментальные средства для анализа рисков и управления
44. рисками. Режим доступу: http://www//ftp.rmcs.department/ess/bss (дата обращения: 10.03.2010 г.).;
45. Міжнародний стандарт ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Звід правил з управління захистом інформації» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=54533;
46. Ларина И.Е. Экономика защиты информации: Учебное пособие. - М.: МГИУ, 2007 - 92 с.;
47. Гладиш С. В. Формування вимог щодо безпеки державних інформаційних ресурсів у телекомунікаційній мережі загального користування // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2012. — № 14. — С. 33–40.;
48. НД ТЗІ 2.5-004- 99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;
49. Максименко Ю.Є. Інформаційні правопорушення: поняття та ознаки // [Електронний ресурс] : Глобальна організація союзницького

лідерства – Режим доступу : http://goal-int.org/informacijni-pravoporushennya-ponyattya- ta-oznaki/ . – 2014;

50. Кримінальний кодекс України [Електронний ресурс]: документ №435-15 від 16.01.2003, ред. 11.06.16. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/435-15;
51. Милославская Н. Г., Управление рисками информационной безопасности: учеб. пособие для вузов. – 2-е изд. [Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.] – М.: Горячая линия-Телеком, 2014. – 130 с. ;
52. Овчинников С.А., Гришин С.Е. Комплексный подход к рассмотрению теории управлением рисками при внедрении информационных технологий // Вестник СГСЭУ. 2011. № 2 (36).;
53. Конеев И.Р. Информационная безопасность предприятия [Конеев И.Р., Беляев А.В.] – СПб.: БХВ-Петербург, – 2003. – 197 с.
54. Grance T., Kent K., Kim B. Computer Security Incident Handling Guide. (NIST SP 800-61). Recommendations of the National Institute of Standards and Technology. — U.S. Department of Commerce, 2004. — http://csrc.nist.gov/publications/nistpubs/800-61/sp800- 61-pdf.zip;
55. Цуркан І.М.. Актуарні розрахунки. Методичні рекомендації до самостійного виконання практичних завдань з дисципліни студентами напряму підготовки 0.030508 Фінанси і кредит / І.М. Цуркан, О.Г. Федорова; М-во освіти і науки України, Нац. гірн. ун-т. – Д. : НГУ, 2014. – 76 с.;
56. Юлдашев Р.Т. Словарь терминов/ Юлдашев Р. Т. — Москва: Анкил, 1999. — 134 с.;
57. Howard J. An Analysis of Security Incidents on the Internet. — CERT/CC, 2000. Електронний ресурс. Режим доступу: http://www.cert.org/research/JHThesis/Start.html;

58. Голов А. Реагирование на инциденты информационной безопасности // Intelligent Enterprise. — 2011. — № 22. — Електронний ресурс. Режим доступу: http://www.topsbi.ru/default.asp?artID=807;
59. Кононович В.Г. Моделювання процесів управління ризиками інформаційної безпеки [Електронний ресурс] / [Кононович В.Г., Копитін Ю.В.] // Управління розвитком складних систем №16, 2013. – с. 100-109. – Режим доступу: http://journals.uran.ua/urss/article/view/38928;
60. Гладиш С. В., Кононович В. Г., Тардаскін М. Ф. Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування //Зв'язок. — 2007. — № 8. — С. 28–31.;
61. НД ТЗІ 2.5.005-99 «Класифікація автоматизованих систем та стандартні функціональні профілі захищеності від НСД» [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407
62. ДСТУ ISO/IEC TR 13335-3:2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT» (ISO/IEC TR 13335-3:1998, IDT) – [Електронний ресурс] – Режим доступу: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005;
63. National Cyber Security Strategy and 2013-2014 Action Plan. – Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications,

2013. – С. 47. – Режим доступу: //www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf;

64. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Електронний ресурс]: документ №24-112/365 від 03.03.2011. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/v0365500-11/;
65. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 1. – С. 312-320.;
66. Про Стратегію кібербезпеки України [Електронний ресурс]: рішення Ради національної безпеки і оборони України №96/2016 від 27.01.2016 року – Режим доступу: http://www.president.gov.ua/documents/962016-19836;
67. Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник / За заг. ред. доктора юридичних наук, професора Р. А. Калюжного. - Запоріжжя: ГУ ЗІДМУ, 2002. - 292 с. ISBN 996-95921-2- 7.;
68. Дослідження витоків конфіденційної інформації у 2015 році компанії InfoWatch [Електронний ресурс] – Режим доступу: http://www.infowatch.ru/report2015;
69. Основи інформаційної безпеки [Електронний ресурс]: навчальний онлайн-курс компанії Zillya! Антивірус – Режим доступу http://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about;
70. Сердюк В.А. Новое в защите от взлома корпоративных систем. – Москва: Техносфера, 2007. – 360 с.];

71. Коваленко Л.П. Стан і перспективи розвитку інформаційно-правової відповідальності / Л. П. Коваленко // Форум права . - 2013. - № 1. - С. 441–445. – Режим доступу:http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_1_76.pdf;
72. Інфографіка про крадіжку грошей в інтернеті [Електронний ресурс]: лабораторія Касперського, 2015. – Режим доступу:http://www.kaspersky.ua/internet-security-center/infographics/stealing-financial-data;
73. Блінова Г.О. Співвідношення правових режимів службової таємниці та персональних даних Форум права». – 2014. – № 1. – С. 39–43 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/jpdf/FP_index.htm_2014_1_8.pdf;
74. Офіційний сайт Міністерства фінансів України [Електронний ресурс] – Режим доступу: http://index.minfin.com.ua/index/infl/;
75. НД ТЗІ 1.3-003- 99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – 30 с.;
76. Максименко Ю.Є., Ліпкан В.А. Засади розвитку інформаційної деліктології / Ю.Є. Максименко, В.А. Ліпкан // Право України. 2013. – №10. – С. 249-256.;
77. Інтернет-магазин «Розетка.УА» [Електронний ресурс] – Режим доступу: http://soft.rozetka.com.ua.;
78. Методичні вказівки до виконання економічної частини дипломного проекту (для студентів напряму підготовки 1701 Інформаційна безпека)/ Упорядн.: О.Г. Вагонова, Ю.О. Волотковська, Н.М. Романюк. – Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2013. – 17 с.;

79. Полушкин А. В. Информационное правонарушение: понятие и виды : дис. … канд. юрид. наук : 12.00.14 / Александр Васильевич Полушкин. — Екатеринбург, 2009. — 223 с.;
80. Ліпкан В., Максименко Ю. Національнобезпекознавство: проблеми формування категорійно-понятійного апарату / В. Ліпкан, Ю. Максименко // Підприємництво, господарство і право. — 2011. — № 8. — С. 7—11.;
81. Резолюции Генеральной Ассамблеи ООН от 30 января 2004 г. по докладу Второго комитета (A/58/481/Add.2)58/199. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур от 23 января 2002 по докладу Третьего комитета (A/56/574) 56/121. Борьба с преступным использованием информационных технологий. http://www:ifap.ru (дата обращения: 23.10.2010 г.).;
82. Овчинников С.А., Гришин С.Е. Формирование культуры кибербезопасности в обществе – актуальная задача современности //Вестник СГСЭУ. 2011. № 3 (37). 206;
83. Максименко Ю.Є. Правове регулювання національної безпеки України: окремі аспекти // Імперативи розвитку юридичної та безпекової науки : матеріали міжнародної науково-практичної інтернет-конференції (Київ, 15 квітня 2010 р.). — К. : О.С. Ліпкан, 2010. — 102 с.;
84. Офіційний сайт Національного банка України [Електронний ресурс] – Режим доступу: http://www.bank.gov.ua/;
85. Овчинников С.А., Семенов В.П. Проблемы стандартизации, совместимости и взаимодействия органов государственной власти, бизнес-процессов и граждан в условиях широкого внедрения информационных технологий // Информационно-

коммуникационные технологии в сфере культуры: сб. мат. Международ. науч.-методич. конф. 19 – 24 сентября, 2011.;

86. Єрохін А.Л. Модель візуалізації нештатних подій у складних інформаційних системах // Зв'язок. — 2009. — № 6. — С. 52–56;

87. Сакович Л.М., Політов В.І. Використання системи підтримки прийняття рішення під час експлуатації та ремонту засобів і комплексів зв'язку // Зв'язок. — 2012. — № 5. — С. 37–39;

88. Коробко В.В., Скоропаденко А.П., Задоя Г.М., Вовк В.М. Интегрированная система сбора информации об экстремальных состояниях телекоммуникационных сетей и их защиты // Зв'язок. — 2011.— № 1. — С. 39–45;

89. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ від 29.03.2006 р. № 373. — 4 с;

90. Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. — Затв. наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р. — 4 с;

91. Dorofee A., Killcrece G., Ruefle R., Zajicek M. Incident Management Capability Metrics. Version 0.1. Technical Report CMU/SEI-2007- TR-008. — CMU, 2007. — 221 p;

92. Мелехин И. Управление инцидентами // Jet Info. — 2011. — № 7. — Електронний ресурс. Режим доступу: http://www.jetinfo.ru/2006/7/3/article3.7.2011.html;

93. Гладиш С.В., Кононович В.Г., Тардаскін М.Ф. Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2013.— № 15. — С. 31–39;

94. Gladysh S. Distribution of responsibility on telecommunication incidents in Ukraine // Матеріали III Міжнародної науково-практичної конференції «Інформаційні технології в наукових дослідженнях і навчальному процесі», Луганськ: ЛНПУ, 2012;
95. ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки»;
96. СБУ : Головні проблеми для України – тероризм і кіберзлочинність // Українська Правда [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/03/23/6961285/;
97. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності //Інформація і право. – 2012. – № 2. – С. 162-169;
98. Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности //Военное право. – 2012. – № 1. – Режим доступу:http://db.inforeg.ru/eni/artList.asp?j=4&id=0220913464&idfull=0421200099;
99. Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, 2010. – 14 c. – Режим доступу : //www.publicsafety.gc.ca/cnt/rsrcs/ pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf;
100. Национальная стратегия кибербезопасности (NCSS). От понимания к возможности.– Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. – Режим доступу: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-cecurity-strategies-ncsss/NCSS2Engelseversie;
101. The Battle for Power on the Internet [Електронний ресурс]. – Режим доступу:

http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power- on-the- internet/280824;

102. Дубов Д. В. Кібербезпека : світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2011. – 30 с.

ДОДАТОК А
ПЕРЕЛІК ФАЙЛІВ НА ЕЛЕКТРОННОМУ НОСІЇ

1 Пояснювальна_записка_Ігнатьєва_125м-16.docx

2 Презентація_до_диплома__Ігнатьєва_125м-16.pptx

ДОДАТОК Б
КОПІЇ НАУКОВИХ ПУБЛІКАЦІЙ

УДК 65.011.3

Ігнатьєва І.Д. студентка групи 125м-16-1
Науковий керівник: Галушко С.О.ст.викладач кафедри БІТ
(Державний ВНЗ “Національний гірничий університет”, м.Дніпро, Україна)

Методи аналізу ризиків для вирішення завдань інформаційної безпеки

Оцінка ризику ІБ є частиною процесу менеджменту ризику і являє собою структурований процес, в рамках якого виявляють способи досягнення поставлених цілей, проводять аналіз наслідків та ймовірності виникнення небезпечних подій для прийняття рішення щодо необхідності обробки ризику. Інакше кажучи, оцінка ризику є процесом, що об'єднує ідентифікацію, аналіз ризику і порівняльну оцінку ризику. Спосіб реалізації цього процесу залежить не тільки від сфери застосування процесу ризик-менеджменту, але також і від методів оцінки ризику. Стандарт ДСТУ IEC/ISO 31010:2013 "Керування ризиком. Методи загального оцінювання ризику" є загальним для всіх областей ризику і призначений для різних цілей організації. Менеджмент ризику допомагає в прийнятті рішень в умовах невизначеності і можливості виникнення подій або обставин (планових і непередбачених), що впливають на досягнення цілей організації.

Стандарт визначає 31 метод аналізу ризиків, з яких і будуть обиратися оптимальні методи для аналізу ризиків інформаційної безпеки. Перерахуємо їх найменування: “Мозкова атака”, “Структуроване чи напівструктуроване опитування”, “Метод Делфі”, “Переліки контрольних

запитань”, “Попереднє аналізування небезпечних чинників (PHA)”, “Дослідження небезпечних чинників і працездатності (HAZOP)”, “Аналізування небезпечних чинників і критичні точки контролю (HACCP), “Загальне оцінюванная екологічного ризику”, “Структурований метод "Що - якщо" (SWIFT)”, “Аналізування сценаріїв”, “Аналізування впливу на діяльність (BIA)”, “Аналізування першопричини (RCA)”, “Аналізування видів і наслідків відмов (FMEA)”, “Аналізування дерева відмов (FTA)”, “Аналізування дерева подій (ETA)”, “Аналізування причин і наслідків”, “Аналізування причинно-наслідкових зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Дерево рішень”, “Загальне оцінювання надійності людини (HRA)”, “Аналізування за схемою "краватка-метелик", “Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Аналізування паразитних схем (SA)”, “Марковське аналізування”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”, “Криві FN”, “Показники ризику”, “Матриця “наслідок-ймовірність”, “Аналізування витрат і вигод (CBA)”, “Багатокритерійне аналізування рішень (MCDA)”.

Завдання вибору методу можна розділити на 2 етапи:

1) вибір придатного методу відповідно до галузі інформаційної безпеки за допомогою оцінки;

2) вибір оптимального методу оцінки ризику.

З вище перелічених методів такі не придатні для аналізу інформаційної безпеки: “Дослідження небезпечних чинників і працездатності (HAZOP)”, “Аналізування небезпечних чинників і критичні точки контролю (HACCP)”, “Загальне оцінюванная екологічного ризику”.

Далі розглянемо методи які стосуються кожного етапу оцінки ризиків. Для ідентифікації ризиків не підходять такі методи: “Аналізування першопричини (RCA)”, “Дерево рішень”, “Аналізування за схемою

"краватка-метелик", “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”. Таким чином, вибір зменшується і тепер вибираємо з 23 методів.

Оптимальність методів розглядається показниками наступних властивостей:

45. ресурсомісткість (необхідні ресурси: тимчасові, інформаційні та інші);

- характеру і ступеня невизначеності оцінки ризику, заснованої на доступній інформації і відповідностям цілям;
- складності проблеми і методів, необхідних для аналізу ризиків.

З таблиці А.2 Додатка А, стандарту ДСТУ IEC/ISO 31010:2013 вибираємо найоптимальніші за наведеними властивостями: “Структуроване опитування”, “Мозковий штурм” та “Переліки контрольних запитань”. Таким чином, для етапу ідентифікації ризику ми вибрали три методи, які можна комбінувати або використовувати найкращий з них.

Для етапу аналізу ризику не підходять такі методи: “Структуроване чи напівструктуроване опитування”, “Переліки контрольних запитань”, “Мозкова атака”, “Метод Делфі”, “Попереднє аналізування небезпечних чинників (PHA)”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”. Таким чином залишається 21 метод. оптимальні з них: “Структурований метод "Що - якщо", “Аналізування впливу на діяльність (BIA)”, “Аналізування першопричини (RCA)”, “Аналізування видів і наслідків відмов (FMEA)”, “Аналізування дерева подій (ETA)”, “Аналізування причинно-наслідкових зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Загальне оцінювання надійності людини (HRA)”, Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Аналізування паразитних схем (SA)”, “Матриця “наслідок-ймовірність”.

Для порівняльної оцінки ризику не підходять такі методи: “Переліки контрольних запитань”, “Структуроване чи напівструктуроване опитування”, “Мозкова атака”, “Метод Делфі”, “Попереднє аналізування небезпечних чинників (PHA)”, “Аналізування дерева подій (ETA)”, “Аналізування причинно-наслідкових зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Аналізування паразитних схем (SA)”, “Марковске аналізування”. З 21 вибираємо оптимальні, грунтуючись також на можливості отримання кількісних вихідних даних: “Аналізування дерева відмов (FTA)”, “Аналізування причин і наслідків”, “Аналізування за схемою "краватка-метелик", “Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”.

Висновок. У цій статті було проведено відбір методів оцінки ризику інформаційної безпеки по кожному етапу загального процесу на базі стандарту ДСТУ IEC/ISO 31010:2013

Практичний досвід побудови моделі загроз інформаційній безпеці виявив, що запропонований підхід значно спрощує завдання застосування методів оцінки ризику для конкретних інформаційних систем і заданого рівня безпеки інформації.

Перелік посилань:

- Смогунов В.В., Вершинин Н.Н., Авдонина Л.А.Классификация методов управления риском // Труды международного симпозиума Надежность и качество. 2009 Т. 2. С. 235-238.
- ДСТУ IEC/ISO 31010:2013

ДОДАТОК В

ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу доц. Волотковська Ю.О.

(підпис) (ініціали, прізвище)