НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій та управління якістю продукції АПК

УДК 006.015.8:004:331.4

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	**Завідувач кафедри**
харчових технологій та управління якістю продукції АПК	стандартизації та сертифікації сільськогосподарської продукції
_____ **Баль-Прилипко Л.В.**	_____ **Толок Г.А.**
«__» _____ 2024 р.	«__» _____ 2024 р.

МАГІСТЕРСЬКА РОБОТА

на тему: «Розроблення елементів системи управління інформаційною безпекою в умовах організації»

Спеціальність: **175 «Інформаційно-вимірювальні технології»**
Освітня програма – **«Якість, стандартизація та сертифікація»**
Орієнтація освітньої програма – **Освітньо-професійна програма**

Гарант освітньої програми
к.т.н., доцент _____ **Слива Ю.В.**

Керівник магістерської роботи
_____ **Антоненко А.В.**
к.т.н., доцент

Виконав _____ **Злобін І.В.**

КИЇВ – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій та управління якістю продукції АПК

ЗАТВЕРДЖУЮ:
Завідувач кафедри
стандартизації та сертифікації сільськогосподарської продукції,
к.т.н., доцент
_____ **Толок Г.А.**
«__» _____ 2024 р.

З А В Д А Н Н Я
ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ
Злобіну Іллі Володимировичу

Спеціальність: 175 «Інформаційно-вимірювальні технології»
Освітня програма – «Якість, стандартизація та сертифікація»
Програма підготовки – Освітньо-професійна
Тема магістерської роботи: «Розроблення елементів системи управління інформаційною безпекою в умовах підприємства»
затверджена наказом ректора НУБіП України № 53 «С» від 17.01.2024 року.

Термін подання завершеної роботи на кафедру 1 листопада 2024 р.

Вихідні дані до магістерської роботи: 1) Положення про підготовку магістрів у НУБіП України; 2) Положення про підготовку і захист магістерської роботи 3) Міжнародні та національні стандарти; 3) Словникові та довідникові джерела; 4) Навчальна та наукова література; 5) Методичні вказівки про підготовку магістерської роботи; 6) Фахові періодичні видання; 7) Матеріали державної статистики; 8) Електронні ресурси.

Перелік питань, що підлягають дослідженню:
1. Аналіз вимог стандартів;
2. Розроблення елементів системи управління інформаційною безпекою в умовах підприємства.
3. Розрахунок економічної ефективності від впровадження передумов.

Дата видачі завдання «26» лютого 2024 р.

Керівник магістерської роботи _____ Антоненко А.В.

Завдання прийняв до виконання _____ Злобін І.В.

РЕФЕРАТ

Магістерська робота, була розроблена з дотриманням усіх вимог та складається з 3 розділів, розміщена на 95 сторінках друкованого тексту, містить 13 таблиць, 9 рисунків, висновки, список використаних джерел та додатки.

В першому розділі роботи досліджено складові та особливі властивості інформаційної безпеки; розглянуто історію ДСТУ ISO/IEC 27001, положення ДСТУ ISO/IEC 27001; досліджено принципи ДСТУ ISO/IEC 27001; розглянуто методи та засоби забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів.

В другому розділі проведена характеристика ТОВ "КБ "ХОРТ", здійснений аналіз діючої інформаційної системи, визначено організаційні заходи забезпечення інформаційної безпеки і захисту інформації підприємства.

В третьому розділі проведено удосконалення засобів захисту інформації на підприємства, здійснено розробку системи інформаційної безпеки підприємства, визначено особливості економічної ефективності розробки системи інформаційної безпеки підприємства.

Ключові слова: *ІНФОРМАЦІЙНА БЕЗПЕКА, РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, , ISO/IEC 27001.*

ЗМІСТ

ДОДАТОК А. Тези І.В. Злобін, Т.В. Науменко, А.В. Антоненко. Розроблення системи управління інформаційною безпекою в умовах організації. XII Міжнародній науково-практичній конференції вчених, аспірантів і студентів «Наукові здобутки у вирішенні актуальних проблем виробництва та переробки сировини, стандартизації і безпеки продовольства» , м. Київ, 18-19 квітня 2024 року: тези доповіді. Київ, 2024. С. 291-292.

ВСТУП

Актуальність теми. Інформаційною безпекою називається комплекс заходів щодо захисту даних від несанкціонованого доступу, руйнувань, модифікацій, розкриттів або затримки при доступі.

В інформаційну безпеку включаються заходи щодо захисту процесу створення інформації, її введення, обробки і виведення. Мета інформаційної безпеки полягає в тому, щоб убезпечити цінність систем, захищати і гарантувати точність і цілісність даних, а також мінімізувати наслідки, які можуть виникнути в тому випадку, коли дані будуть модифіковані або зруйновані.

В рамках інформаційної безпеки потрібно облік всіх дій, в ході яких інформація створюється, піддається модифікації, коли до неї здійснюється доступ або вона поширюється по мережі.

Це універсальне поняття застосовується незалежно від форми, яку можуть приймати дані (електронна або, наприклад, фізична). Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації.

Сучасна та ефективна система забезпечення інформаційної безпеки (СЗІБ) являє собою комплекс заходів, спрямованих на захист конфіденційної корпоративної інформації на всіх стадіях її життєвого циклу: в процесі обробки, передачі, зберігання.

Це особливо важливо для організацій з територіально розподіленою інфраструктурою, в який здійснюється безперервний обмін даними між окремими підрозділами та регіональними представництвами.

СЗІБ в повній мірі виконує свої функції, тільки якщо є ретельно спланованою, налагодженою системою, в діяльності якої використовуються передові технології та дотримуються міжнародні стандарти інформаційної безпеки. Саме такий підхід повинні здійснювати організації України при створенні,

впровадженні та супроводі СЗІБ в організаціях будь-яких масштабів і сфер діяльності.

Безперервне функціонування СЗІБ відбувається завдяки поєднанню організаційних і технічних заходів, що застосовуються відповідно до управлінських рішень, які розробляються в рамках системи управління інформаційною безпекою (СУІБ).

При створенні сучасних СЗІБ розробники повинні діяти у відповідності зі стандартами, що описують основні етапи проектування та впровадження автоматизованих систем.

Таким чином, створення СЗІБ – це комплексний підхід до захисту конфіденційної корпоративної інформації із залученням кваліфікованих спеціалістів та експертів. При цьому проекти повинні (можуть) розроблятися і реалізуватися відповідно до міжнародних стандартів інформаційної безпеки, а також з урахуванням кращих світових практик та думок експертів сучасного IT ринку.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури свідчить, що питання системи інформаційної безпеки досліджували в своїх наукових роботах такі вчені, як: Швець В.А., Шестакова В.В., Львова А.В., Маслова М.А., Герасименко В.А., Малюк А.А. та деякі інші. Однак питаняя розробки системи інформаційної безпеки підприємства до сьогоднішнього дня все ще залишається без належної уваги вчених.

Мета і завдання дослідження. Мета дипломної роботи полягає в тому, щоб на основі критичного розгляду нормативних актів, монографічних, літературних джерел, інтернет здійснити розроблення елементів системи управління інформаційною безпекою в умовах підприємства ТОВ "КБ "ХОРТ".

Відповідно до визначеної мети було поставлено такі завдання:

– дослідити складові та особливі властивості інформаційної безпеки;

– розглянути історію ISO/IEC 27001.

– розглянути положення ISO/IEC 27001.

– дослідити принципи ISO/IEC 27001.

– розглянути методи та засоби забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів.

– провести характеристику ТОВ "КБ "ХОРТ".

– провести аналіз діючої інформаційної системи.

– визначити організаційні заходи забезпечення інформаційної безпеки і захисту інформації підприємства.

– провести удосконалення засобів захисту інформації на підприємстві.

– провести розробку системи інформаційної безпеки підприємства.

– визначити особливості економічної ефективності розробки системи інформаційної безпеки підприємства.

Об'єктом дослідження є інформаційна безпека.

Предметом дослідження є розроблення елементів системи управління інформаційною безпекою в умовах підприємства ТОВ "КБ "ХОРТ".

Методи дослідження. Методологічну основу дослідження склали наступні методи пізнання: аналіз, синтез, індукція і дедукція, методи матеріалістичної діалектики узагальнення, системний підхід, порівняльний аналіз.

Теоретична, методична та практична значущість отриманих результатів. Магістерська робота являє собою монографічне дослідження, присвячене комплексному аналізу розроблення елементів системи управління інформаційною безпекою в умовах підприємства ТОВ "КБ "ХОРТ". Автором здійснено розробку цілого ряду теоретичних положень, сукупність яких може бути кваліфікована як рішення багатьох проблем – досліджено складові та особливі властивості інформаційної безпеки; проаналізовано сімейство стандартів ISO/IEC 27001; проведено аналіз методів та засобів забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів. Практичне значення результатів проведеного дослідження полягає у тому, що аналіз та обґрунтовані положення, викладені в роботі, можуть бути реалізовані для

студентів економічних факультетів, факультетів менеджменту та інших. Результати дослідження можуть використовуватися при теоретичній та практичній роботі, яка пов’язана з дослідженням системи інформаційної безпеки.

Інформаційна база дослідження. Інформаційна база представлена нормативно-правовими актами, законами, монографіями, авторськими статтями та інформаційними сайтами мережі Інтернет.

РОЗДІЛ І. ОГЛЯД ЛІТЕРАТУРИ

1.1 Складові та особливі властивості інформаційної безпеки

На даний момент до продуктів інформаційної безпеки відноситься великий спектр найрізноманітніших рішень, включаючи систему збору кореляції подій, аналітичні системи, системи контролю за витоками і так далі.

І якщо ми подивимося всередину цих систем, то ми побачимо, що вони містять в собі чималий функціонал або IT-систем, або систем оптимізації процесів. Це одна з принципових тенденцій, що склалася.

У сучасному вигляді інформаційна безпека почала формуватися 20-25 років тому, тоді ж вона являла собою роботу із засобами захисту. Тобто спочатку у нас з'явилися засоби захисту інформації, які необхідно було адмініструвати, ними потрібно було керувати, і перші служби інформаційної безпеки займалися саме такою роботою. Це міжмережеві екрани, засоби антивірусного захисту, пізніше з'явилися засоби виявлення вторгнень і так далі [1].

Потужний поштовх у напрямку розвитку систем управління стався 10 років тому, з появою тематики захисту персональних даних. Це призвело до того, що інформаційна безпека стала сприйматися не тільки як робота із засобами захисту, а як процес, яким необхідно управляти. З'явилися закони, стандарти, вимоги регуляторів, які активно стали застосовуватися на обов'язковому рівні і підтримуватися законодавством.

Поступово від роботи із засобами захисту перейшли до епохисистем менеджменту. І для цього з'явилися відповідні продукти, які дозволяють все це реалізувати. Озираючись на класичну історію, це міжмережеві екрани, засоби антивірусного захисту, проте в сучасних реаліях в великих організаціях це такі системи і підсистеми як антивірусний захист та інші засоби, які перейшли на адміністрування звичайних служб IT [2].

Як результат, служби інформаційної безпеки набули функцію контролю, а саме функцію контролю і управління певною частиною деяких процесів. Наприклад, щоб встановити який-небудь додаток, необхідна заявка проходить, в числі іншого, і службу безпеки.

Різні підрозділи, які існують в сучасних компаніях, закріплюють за собою функцію інформаційної безпеки. Наприклад, системи, якими користуються сучасні служби економічної безпеки або служби фізичної безпеки, тепер нерозривно пов'язані з інструментарієм ринку інформаційної безпеки.

Люди, що займаються конкурентної розвідкою, також використовують системи, якими користуються служби інформаційної безпеки. У той же час служби інформаційної безпеки користуються системами служб економічної безпеки. Ми стаємо свідками ситуації, коли розмиваються межі між різними службами.

Інформаційна безпека перестала бути окремою службою, вона стала окремою функцією. Сьогодні, коли організація створює або купує якусь інформаційну систему, вона не хоче займатися забезпеченням її безпеки. Вона хоче або купити безпечну систему, яка відповідає її критеріям, або ж створити безпечну систему [3].

Якщо ми подивимося на групи розробки, існуючі в великих компаніях сьогодні, то розробкою продуктів займаються невеликі команди, в яких є люди, які відповідають за окремі питання інформаційної безпеки, наприклад, щодо безпеки розробки; окремі фахівці займаються питаннями коректності вбудовування криптографії; інші розбираються в регуляторних питаннях у напрямку конкретного продукту.

Інформаційна безпека перетворилася в функцію, яку можна замінити окремими учасниками команди. Тепер, якщо ми подивимося на великих розробників програмних продуктів - «Яндекс» або «Google», то ми побачимо, що розподіл йде по продуктовим лінійкам.

Розробкою конкретного продукту займаються не тільки розробники, програмісти, але також є люди, які займаються питаннями інформаційної безпеки в рамках цього продукту.

Якщо розглянути кожного окремо: буде 100 продуктів, буде 100 функцій в кожному продукті з питань інформаційної безпеки. Якщо ми подивимося на сучасні українські компанії, то в структурі менеджменту обов'язково є людина, що розбирається в питаннях інформаційної безпеки.

Якщо ми подивимося на правову сторону питання, знову ж таки - юридичні служби так само набирають людей, які займаються або принаймні на якомусь рівні розбираються в питаннях інформаційної безпеки і в стані проконсультувати з цих питань [4].

Питання інформаційної безпеки в сучасній Україні стоїть так само гостро, як і питання динамічного економічного розвитку і інтеграції в світову спільноту. Інформація, поряд з фінансовими та природними ресурсами, є найважливішим чинником конкурентоспроможності країни на міжнародній арені.

До недавнього часу проблемам інформаційної безпеки всередині країни і в зовнішньому просторі приділялося вкрай мало уваги. У зв'язку з цим в останні роки органами законодавчої і виконавчої влади України були прийняті закони і підзаконні акти з питань захисту державної таємниці, забезпечення збереження інформаційних ресурсів держави, їх раціонального використання, регламентації міжнародного інформаційного обміну.

До українських законів, що регулюють інформаційну безпеку в нашій країні відносяться: Конституція України [5], закон «Про державну таємницю» [6], закон «Про захист інформації в інформаційно-телекомунікаційних системах» [7], закон «Про інформацію» [8] і т.д.

На думку одних фахівців «інформаційна безпека» це:

- стан захищеності інформаційного простору, що забезпечує його формування і розвиток в інтересах громадян, організацій і держави;

- стан інфраструктури системи (об'єкта, держави), при якому інформація використовується суворо за призначенням і не робить негативного впливу на систему (об'єкт, держава) при її використанні;

- стан інформації, при якому виключається або суттєво ускладнюється порушення таких її властивостей, як секретність, цілісність [9].

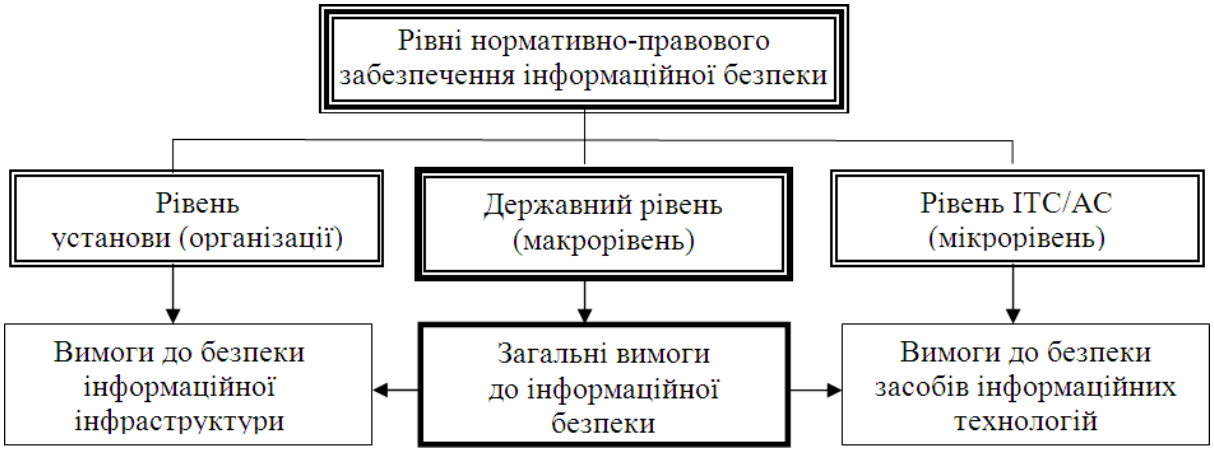

Рис. 1.1 Рівні нормативно-правового забезпечення інформаційної безпеки

Інформаційна безпека - практика запобігання несанкціонованому доступу, використання, розкриття, спотворення, зміни, дослідження, записи або знищення інформації.

Це універсальне поняття застосовується незалежно від форми, яку можуть приймати дані (електронна або, наприклад, фізична). Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації.

Це досягається, в основному, за допомогою багатоетапного процесу управління ризиками, який дозволяє ідентифікувати основні засоби та нематеріальні активи, джерела загроз, уразливості, потенційну ступінь впливу і можливості управління ризиками. Цей процес супроводжується оцінкою ефективності плану з управління ризиками [10].

Для того, щоб стандартизувати цю діяльність, наукові і професійні спільноти знаходяться в постійному співробітництві, спрямованому на вироблення базової методології, політик і індустріальних стандартів в галузі технічних заходів захисту інформації, юридичної відповідальності, а також стандартів навчання користувачів і адміністраторів.

Ця стандартизація значною мірою розвивається під впливом широкого спектра законодавчих і нормативних актів, які регулюють способи доступу, обробки, зберігання та передачі даних. Однак впровадження будь-яких стандартів і методологій в організації може мати лише поверхневий ефект, якщо культура безперервного вдосконалення не закріплена належним чином [11].

Рис. 1.2 Принципи інформаційної безпеки

В інформаційній безпеці повинні бути чітко позначені два її складових аспекти:

1. Інформаційно-технічний - захист, контроль і дотримання законності та правопорядку в телекомунікаційній сфері (захист від: несанкціонованого доступу, хакерських зломів комп'ютерних мереж і сайтів, логічних бомб, комп'ютерних вірусів і шкідливих програм, несанкціонованого використання частот, радіоелектронних атак і ін.);

2. Інформаційно-психологічний захист психіки суспільства і держави від негативного інформаційного впливу.

Іншими словами, пріоритетним завданням держави у сфері інформаційної безпеки, є захист інформації від несанкціонованої обробки з метою впливу на процес прийняття рішення окремою особистістю або суспільством в цілому [12].

В основі інформаційної безпеки лежить діяльність по захисту інформації - забезпечення її конфіденційності, доступності та цілісності, а також недопущення будь-якої компрометації в критичній ситуації.

До таких ситуацій належать природні, техногенні і соціальні катастрофи, комп'ютерні збої, фізичне викрадення і тому подібні явища. У той час, як діловодство більшості організацій в світі досі базується на паперових документах, що вимагають відповідних заходів забезпечення інформаційної безпеки, спостерігається неухильне зростання числа ініціатив по впровадженню цифрових технологій на підприємствах, що тягне за собою залучення фахівців з безпеки інформаційних технологій (IT) для захисту інформації.

Ці фахівці забезпечують інформаційну безпеку технології (в більшості випадків - будь-якої різновиди комп'ютерних систем). Слід зазначити, що під комп'ютером в даному контексті мається на увазі не тільки побутової персональний комп'ютер, а цифрові пристрої будь-якої складності і призначення, починаючи від примітивних і ізольованих, на зразок електронних калькуляторів і побутових приладів, аж до індустріальних систем управління і суперкомп'ютерів, об'єднаних комп'ютерними мережами [13].

Найбільші підприємства і організації, в силу життєвої важливості і цінності інформації для їхнього бізнесу, наймають фахівців з інформаційної безпеки, як правило, собі в штат. В їх завдання входить убезпечити всі технології від шкідливих кібератак, найчастіше націлених на викрадення важливої конфіденційної інформації або на перехоплення управління внутрішніми системами організації.

Інформаційна безпека, як сфера зайнятості, значно розвинулася і виросла в останні роки. У ній виникло безліч професійних спеціалізацій, наприклад, таких, як безпека мереж і пов'язаної інфраструктури, захисту програмного забезпечення та баз даних, аудит інформаційних систем, планування безперервності бізнесу, виявлення електронних записів і комп'ютерна криміналістика.

До загроз інформаційної безпеки слід віднести:

- загрози конституційним правам і свободам людини і громадянина у сфері духовного життя та інформаційної діяльності, індивідуальному, груповому та суспільному свідомості, духовному відродженню держави;

- загрози інформаційного забезпечення державної політики;

- загрози розвитку вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікації і зв'язку, забезпечення потреб внутрішнього ринку в її продукції і виходу цієї продукції на світовий ринок, а також забезпечення накопичення, збереження і ефективного використання вітчизняних інформаційних ресурсів;

- загрози безпеки інформаційних і телекомунікаційних засобів і систем [14].

Загрози інформаційної безпеки можуть приймати вельми різноманітні форми. На 2019 рік найбільш серйозними вважаються загрози пов'язані з «злочином як послугою», Інтернетом речей, ланцюгами поставок і ускладненням вимог регуляторів [15].

«Злочин як послуга» є модель надання зрілими злочинними співтовариствами пакетів кримінальних послуг на даркнет-ринку за доступними цінами

початківцям-кіберзлочинцям. Це дозволяє останнім здійснювати хакерські атаки, раніше недоступні через високу технічну складність або дорожнечі, роблячи кіберзлочинність масовим явищем [15].

Організації активно впроваджують Інтернет речей, пристрої якого часто спроектовані без урахування вимог безпеки, що відкриває додаткові можливості для атаки. До того ж, швидкий розвиток і ускладнення Інтернету речей знижує його прозорість, що в поєднанні з нечітко визначеними правовими нормами і умовами дозволяє організаціям використовувати зібрані пристроями персональні дані своїх клієнтів на власний розсуд без їх відома.

Крім того, для самих організацій проблематично відстежувати, які із зібраних пристроями Інтернету речей даних передаються у поза. Загроза ланцюгів поставок полягає в тому, що організації, як правило, передають своїм постачальникам різноманітну цінну і конфіденційну інформацію, в результаті чого втрачають безпосередній контроль над нею [16].

Таким чином, значно зростає ризик порушення конфіденційності, цілісності або доступності цієї інформації.

Все нові і нові вимоги регуляторів значно ускладнюють управління життєво-важливими інформаційними активами організацій. Наприклад, введений в дію в 2018 році в Євросоюзі Загальний регламент захисту персональних даних, вимагає від будь-якої організації в будь-який момент часу на будь-якій ділянці власної діяльності або ланцюга поставок, продемонструвати, які персональні дані і для з якою метою є там в наявності, як вони обробляються, зберігаються і захищаються [17].

Причому ця інформація повинна бути надана не тільки в ході перевірок уповноваженими органами, а й на першу вимогу приватної особи - власника цих даних. І хоча впорядкування обробки персональних даних передбачає в довгостроковій перспективі поліпшення інформаційної безпеки, в короткостроковому плані ризики організації помітно зростають.

Органи державної влади, збройні сили, корпорації, фінансові інститути, медичні установи і приватні підприємці постійно накопичують значні обсяги

конфіденційної інформації про своїх співробітників, клієнтів, продуктах, наукових дослідженнях і фінансові результати. Попадання такої інформації в руки конкурентів або кіберзлочинців може спричинити для організації та її клієнтів далекосяжні юридичні наслідки, непоправні фінансові та репутаційні втрати.

Основними способами протидії загрозам інформаційної безпеки або інформаційним ризикам є:

- зниження - впровадження заходів безпеки і протидії для усунення вразливостей і запобігання загрозам;

- передача - перенесення витрат, пов'язаних з реалізацією загроз на третіх осіб: страхові або аутсорсингові компанії;

- прийняття - формування фінансових резервів у разі, якщо вартість реалізації заходів безпеки перевищує потенційний збиток від реалізації загрози;

- відмова - відмова від надмірно ризикованої діяльності [18].

Системний підхід до опису інформаційної безпеки пропонує виділити наступні складові інформаційної безпеки [19]:

1. Законодавча, нормативно-правова та наукова база.

2. Структура і завдання органів (підрозділів), що забезпечують безпеку ІТ.

3. Організаційно-технічні та режимні заходи і методи (Політика інформаційної безпеки).

4. Програмно-технічні засоби і способи забезпечення інформаційної безпеки.

Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту (СЗІБ). Для побудови та ефективної експлуатації СЗІБ необхідно:

– виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;

– врахувати вимоги національного та міжнародного законодавства;

– використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ;

– визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ;

– розподілити між підрозділами області відповідальності в здійсненні вимог СЗІБ;

– на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові Політику інформаційної безпеки об'єкта захисту;

– реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-апаратні, інженерно-технічні та інші способи і засоби захисту інформації;

– реалізувати систему менеджменту (управління) інформаційної безпеки.

Як видно з останнього етапу робіт, процес реалізації СЗІБ безперервний і циклічно (після кожного перегляду) повертається до першого етапу, повторюючи послідовно всі інші. Так СЗІБ коригується для ефективного виконання завдань захисту інформації та відповідності новим вимогам, що постійно оновлюється інформаційної системи.

Організаційний захист - це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз. Організаційна захист забезпечує: організацію охорони, режиму, роботу з кадрами, з документами; використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх і зовнішніх загроз підприємницької діяльності [20].

До основних організаційних заходів можна віднести:

– організацію режиму і охорони. Їх мета - виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб;

– організацію роботи з співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення з співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;

– організацію роботи з документами і документованої інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;

– організацію використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;

– організацію роботи з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації і вироблення заходів щодо забезпечення її захисту;

– організацію роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання і знищення документів і технічних носіїв [21].

У кожному конкретному випадку організаційні заходи носять специфічну для даної організації форму і зміст, спрямовані на забезпечення безпеки інформації в конкретних умовах.

Інформаційна безпека підприємства - це стан захищеності корпоративних даних, при якій забезпечується їх конфіденційність, цілісність, автентичність і доступність.

Завдання систем інформаційної безпеки підприємства різні:

– забезпечення захищеного зберігання інформації на носіях;

– захист даних, що передаються по каналах зв'язку;

– створення резервних копій, післяаварійне відновлення і т. д.

Забезпечення інформаційної безпеки підприємства можливо тільки при системному і комплексному підході до захисту.

Повноцінна інформаційна безпека має на увазі безперервний контроль всіх важливих подій і станів, що впливають на безпеку даних і здійснюється цілий рік [22].

Інформаційна безпека підприємства досягається цілим комплексом організаційних і технічних заходів, спрямованих на захист корпоративних даних. Організаційні заходи включають задокументовані методики та правила роботи з різними видами інформації, IT-сервісами, засобами захисту і т. д.

Технічні заходи полягають у використанні апаратних і програмних засобів контролю доступу, моніторингу витоків, антивірусного захисту, міжмережевого екранування, захисту від електромагнітних випромінювань і інше [23].

Забезпечення інформаційної безпеки - це безперервний процес, що включає в себе, п'ять ключових етапів:

– оцінка вартості;
– розробка політики безпеки;
– реалізація політики;
– кваліфікована підготовка фахівців;
– аудит.

З оцінки майна починається процес забезпечення інформаційної безпеки, визначення інформаційних активів організації, факторів, що загрожують цій інформації, і її уразливості, значущості загального ризику для організації. Залежно від майна і буде складатися програма захисту цих активів. Після того, як ризик буде виявлений і буде складена його кількісна оцінка, можна буде вибрати рентабельну контрзахід для зменшення цього ризику.

Цілі оцінки інформаційної безпеки:

– визначити цінність інформаційних активів;
– визначити загрози для конфіденційності, цілісності, доступності та / або можуть бути ідентифіковані цих активів;
– визначити існуючі вразливі місця в практичній діяльності організації;

– встановити ризики організації щодо інформаційних активів;

– запропонувати зміни в існуючій практиці роботи, які дозволять скоротити величину ризиків до допустимого рівня;

– забезпечити базу для створення проекту забезпечення безпеки [24].

П'ять основних видів оцінки:

1. Оцінка вразливих місць на системному рівні. Комп'ютерні системи досліджені на відомі уразливості і найпростіші політики відповідності технічним вимогам.

2. Оцінка на мережевому рівні. Зроблено оцінку існуючої комп'ютерної мережі та інформаційної інфраструктури, виявлені зони ризику.

3. Загальна оцінка ризику в рамках організації. Зроблено аналіз всієї організації з метою виявлення загроз для її інформаційних активів.

4. Аудит. Досліджено існуюча політика і відповідність організації цієї політики.

5. Випробування на можливість проникнення.

При проведенні оцінки повинні бути досліджені такі документи, як:

– політика безпеки;

– інформаційна політика;

– політика і процедури резервного копіювання;

– довідкове керівництво працівника або інструкції;

– процедури найму-звільнення працівників;

– методологія розробки програмного забезпечення;

– методологія зміни програмного забезпечення;

– телекомунікаційні політики;

– діаграми мережі [25].

Отримавши вищевказані політики і процедури, кожна з них досліджується на предмет значущості, правомірності, завершеності і актуальності, так як політики і процедури повинні відповідати меті, визначеній в документі.

Після оцінки необхідно зайнятися розробкою політик і процедур, які визначають передбачуваний стан безпеки і перелік необхідних робіт. Ні політики - немає плану, на підставі якого організація розробить і виконає ефективну програму ДБЖ.

Необхідно розробити такі політики і процедури:

1. Інформаційна політика. Виявляє секретну інформацію і способи її обробки, зберігання, передачі та знищення.

2. Політика безпеки. Визначає технічні засоби управління для різних комп'ютерних систем.

3. Політика використання. Забезпечує політику компанії по використанню комп'ютерних систем.

4. Політика резервного копіювання. Визначає вимоги до резервних копій комп'ютерних систем.

5. Процедури управління обліковими записами. Визначають дії, що виконуються при додаванні або видаленні користувачів.

6. План на випадок надзвичайних обставин. Забезпечує дії по відновленню обладнання компанії після стихійних лих або інцидентів, що сталися з вини людини [26].

Реалізація політики безпеки полягає в реалізації технічних засобів та засобів безпосереднього контролю, а також в підборі штату безпеки. Можуть знадобитися зміни в конфігурації систем, що знаходяться поза компетенцією відділу безпеки, тому в проведенні програми безпеки повинні брати участь системні і мережеві адміністратори.

При застосуванні будь-яких нових систем безпеки потрібно мати у своєму розпорядженні кваліфікованим персоналом. Організація не може забезпечити захист секретної інформації, не привертаючи своїх співробітників. Грамотна професійна перепідготовка - це механізм забезпечення співробітників необхідною інформацією.

Співробітники повинні знати, чому питання безпеки так важливі, повинні бути навчені виявлення і захист секретної інформації.

Аудит - це останній крок в процесі реалізації інформаційної безпеки. Він визначає стан інформаційної безпеки всередині організації, створення відповідних політик і процедур, приведення в дію технічних засобів контролю і навчання персоналу.

1.2 Сімейство стандартів ISO/IEC 27001

1.2.1 Історія ISO/IEC 27001

У 1992 р Міністерство торгівлі і промисловості Великобританії опублікувало Кодекс управління інформаційною безпекою (Code of Practice for Information Security Management). Розробники кодексу не могли собі уявити, що їх документ в майбутньому ляже в основу двох міжнародних стандартів, яким будуть слідувати тисячі організацій по всьому світу.

У 1995 р Британський інститут стандартів (BSI) прийняв Кодекс управління інформаційною безпекою в якості національного стандарту Великобританії і зареєстрував його під номером BS7799.

У 1998 р BSI публікує стандарт BS7799-2. У стандарті була представлена процедура вдосконалення заходів забезпечення ІБ, описаних в BS7799, відповідно до циклом Демінга (Plan - Do - Check - Act), а також системний підхід до управління заходами.

У 2000 р британський стандарт BS7799 був адаптований під вимоги Міжнародної організації зі стандартизації (ISO) і виданий під номером ISO / IEC 17799.

У 2005 р BS7799-2 стає Міжнародним стандартом ISO / IEC 27001: 2005.

У 2007 р стандарт ISO / IEC 17799 був включений в лінійку стандартів 27-й серії і отримав новий номер - ISO / IEC 27002: 2005.

З 2005 р сертифікаційний аудит на відповідність вимогам стандарту ISO / IEC 27001: 2005 пройшло більше 17 тис. Компаній по всьому світу (за даними BSI). Ще більше компаній не подавали заявок на проведення сертифікаційного

аудиту, але використовували стандарт в якості джерела кращих практик при проектуванні систем управління ІБ [27].

За 8 років технології пішли вперед і деякі заходи безпеки зараз вже недостатні. Наприклад, вимога щодо перевірки даних, що вводяться, необхідне для мінімізації ризику SQL-ін'єкцій, в даний час є лише невеликою частиною захисту від хакерських атак, і даний контроль вже не може самостійно забезпечити помітне зниження ризику.

Стандарт включає кілька вимог, які є окремими випадками інших вимог. Наприклад, міра "захист системної документації" має на увазі, що ми повинні приділити їй особливу увагу, однак, за своєю суттю, системна документація є таким же інформаційним активом, як і будь-яка інша інформація, для якої в ході інвентаризації активів і оцінки ризиків визначені вимоги по захисту.

В ході приведення у відповідність стандарту BS7799-2 вимогам ISO міру "запобігання неналежного використання систем обробки даних", що є вимогою британського законодавства, помилково залишили в стандарті.

Однак необхідності в ній немає, так як міра "Визначення всіх застосовних договірних вимог і вимог законодавства" успішно її закриває.

Крім того, за останні кілька років були оновлені стандарти, з якими гармонізований ISO / IEC 27001: 2005, а також був розроблений ряд допоміжних стандартів 27-й серії.

З цих причин стало очевидно - стандарту необхідний перегляд. У 2010 р з'явилася перша інформація, що попередня версія нової редакції стандарту вже обговорюється в BSI і очікується до опублікування в 2013 р.

Фахівці з ІБ усього світу стежили за новинами з закритих обговорень в стінах BSI, щоб дізнатися, які зміни вимог найімовірніше з'являться в стандарті.

Необхідно було спрогнозувати, наскільки складно буде виконати нові вимоги, і зрозуміти, що робити тим, хто вже пройшов сертифікаційний аудит по застарілої версії стандарту.

В початку 2013 р попередні версії стандартів ISO / IEC 27001 та ISO / IEC 27002 були опубліковані на сайті BSI для публічного обговорення. Тепер ми можемо оцінити, в якому напрямку розвиваються стандарти, і постараємося відповісти на виникаючі в зв'язку з цим питання [28].

Перше, що кидається в очі при аналізі запропонованих змін нової редакції стандарту, - це його структура, яку ми вже бачили в ISO 22301: 2012 "Вимоги до систем управління безперервністю бізнесу".

Дивлячись на оновлену структуру, складається враження, що текст стандарту також зазнав значних змін, проте це не зовсім так - при більш детальному вивченні стає зрозуміло, що вимоги були просто перенесені з одних розділів старої редакції в інші розділи нової, а крім того, були вилучені дублюються вимоги.

У 2011 р був випущений стандарт ISO / IEC 27005: 2011, детально розкриває дану тему, тому зі стандарту було виключено детальний опис рекомендованого підходу до оцінки ризиків.

Тепер компанія може самостійно вибирати підходящу методологію (метод "актив - загроза - вразливість" залишиться як найкраща практика для цього стандарту) і це не позначиться на результатах проведення оцінки. Крім того, зі стандарту пропав термін "власник активу" (asset owner), замість нього використовується термін "власник ризику" (risk owner).

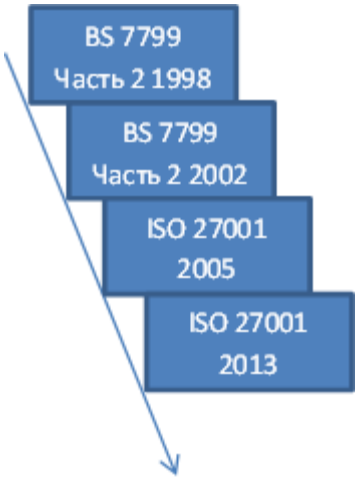

Рис. 1.3 Розвиток до ISO 27001:2013

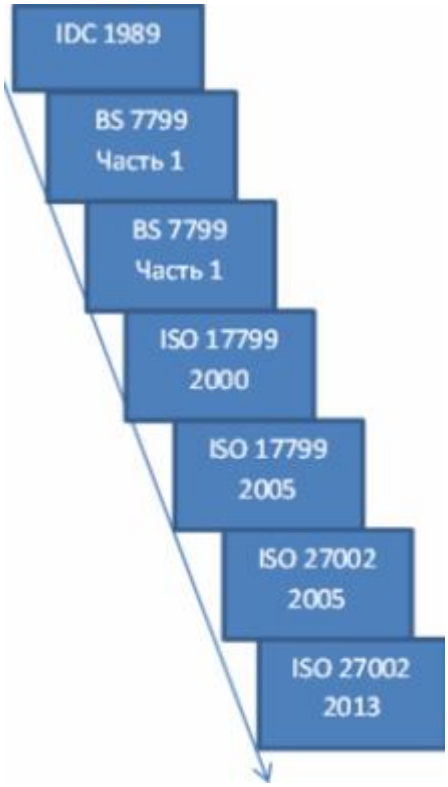

Рис. 1.4 Розвиток до ISO 27002:2013

Оновлений стандарт враховує інтереси всіх сторін, що взаємодіють з організацією (акціонерів, регуляторів, клієнтів, партнерів) і дозволяє визначити окремі вимоги для кожного з них.

Нова вимога стандарту, що стосується необхідності визначення переліку осіб (всередині і поза організації), з якими необхідно взаємодіяти з питань, пов'язаних з управлінням ІБ. Тепер компанія повинна визначити інформацію, яку необхідно довести до відома зацікавлених осіб, а також коли, хто і як повинен це робити. З введенням такої процедури має спроститися залучення керівництва і власників бізнес-процесів в управління ІБ, так як тепер вони можуть отримувати всю актуальну інформацію, що стосується функціонування системи управління ІБ.

27-я серія стандартів активно розвивається - за вісім років було випущено 16 додаткових стандартів. Оновлення ISO / IEC 27001 та ISO / IEC 27002 в цьому році - це всього лише черговий рубіж, який до кінця року подолають

розробники серії. На найближчі два роки в BSI заплановані наступні оновлення і видання нових стандартів:

ISO / IEC 27014 "Управління ІБ вищим керівництвом". В даний час стандарт знаходиться на фінальній стадії розробки і, найімовірніше, буде опублікований в самий найближчий час.

ISO / IEC 27011 "Управління ІБ для телекомунікаційних компаній". Даний стандарт є галузевої версією ISO / IEC 27002, тому він буде оновлений в найкоротші терміни відразу після публікації фінальної версії даного стандарту.

ISO / IEC 27004 "Метрики ІБ". Перша редакція стандарту була опублікована в 2009 році і в даний час знаходиться на стадії перегляду в BSI [29].

В цілому нова версія стандарту залишає приємне враження:

Стандарт сприяє більшому залученню до процесів управління ІБ керівництва організації і дає в руки інструмент, який дозволить ефективніше взаємодіяти топ-менеджменту і особам, відповідальним за ІБ.

Деякі вимоги стандарту стали менш жорсткими, що дає велику гнучкість для компанії у виборі методик і захисних заходів.

Вимоги та заходи попередньої версії були істотно оптимізовані, таким чином, багато спірні моменти будуть подолані.

Гармонізація з усіма сучасними стандартами, випущеними Міжнародною організацією зі стандартизації, дозволить компаніям інтегрувати свої системи управління ІБ в існуючі процеси найбільш ефективно. Природно, якщо процеси побудовані на методологіях стандартів ISO.

1.2.2 Огляд ISO/IEC 27001

ISO / IEC 27001 - міжнародний стандарт по інформаційної безпеки, розроблений спільно Міжнародною організацією зі стандартизації та Міжнародної електротехнічної комісією.

Підготовлен до випуску підкомітетом SC27 Об'єднаного технічного комітету JTC 1. Стандарт містить вимоги в області інформаційної безпеки для створення, розвитку та підтримки Системи менеджменту інформаційної безпеки (СМІБ).

ISO 27001 може бути впроваджений в будь-якій організації: комерційної або некомерційної, приватної або державної, маленької чи великої. Він був написаний провідними світовими експертами в області інформаційної безпеки і пропонує методологію для впровадження управління інформаційною безпекою на підприємстві.

Він також дозволяє компаніям отримати сертифікацію, що означає, що незалежний орган із сертифікації підтвердить, що організація впровадила інформаційну безпеку відповідно до стандарту ISO 27001 [29].

У стандарті ISO / IEC 27001 (ISO 27001) зібрані описи найкращих світових практик в області управління інформаційною безпекою. ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення Системи Менеджменту Інформаційної Безпеки (СМІБ).

Мета СМІБ - вибір відповідних заходів управління безпекою, призначених для захисту інформаційних активів і гарантують довіру зацікавлених сторін.

Саме поняття «захисту інформації» трактується міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації. Основа стандарту ICO 27001 - система управління ризиками, пов'язаними з інформацією. Система управління ризиками дозволяє отримувати відповіді на наступні питання:

– на якому напрямку інформаційної безпеки потрібно зосередити увагу;

– скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації.

Структура Стандарту ISO / IEC 27001: 2005:

– Передмова
– Вступ
– Область застосування
– Нормативні посилання
– Терміни та визначення
– Система менеджменту захисту інформації
– Відповідальність керівництва
– Внутрішні аудити СМІБ
– Аналіз СМІБ з боку керівництва
– Поліпшення СМІБ
– Додаток А (обов'язковий) цілі управління і засоби управління
– Додаток В (довідковий) принципи OECD і цей міжнародний стандарт
– Додаток С (інформаційне) відповідність між ISO 9001: 2000, ISO 14001: 2004 та цим міжнародним стандартом
– Бібліографія [28].

У 2013 році Міжнародною організацією по сертифікації була розроблена і прийнята нова версія стандарту ISO / IEC 27001 до: 2013. Зміни торкнулися як структури стандарту, так і вимог.

Структура основних вимог стандарту ISO / IEC 27001 до: 2013 приведена у відповідність до Директив ISO / IEC (тобто всі стандарти міжнародної організації матимуть ідентичну структуру розділів). На російську мову дана версія стандарту ще не переведена, але англійський варіант текстового вмісту нового стандарту такий:

1. Introduction
2. Scope

3. Normative references
4. Terms and definitions
5. Context of organization
6. Leadership
7. Planning
8. Support
9. Operation
10. Performance evaluation
11. Improvement [27].

Також відбулися зміни в структурі Додатка «А» стандарту. З'явилися три нові розділи:

– «А.10 Криптографія»,
– «А.13 Безпека комунікацій»,
– «А.15 Взаємовідносини з постачальниками».

Розділ «А.10 Криптографія» не є новим, його вимоги повторюють окремі пункти розділу А.12 старої версії стандарту.

Розділи «А.13 Безпека комунікацій» і «А.15 Взаємовідносини з постачальниками» зібрали окремі пункти по розділах Програми «А» версії 2005, а також включили деякі нові вимоги.

Зміни в основній частині нової версії стандарту ISO / IEC 27001 до: 2013:

– чітко сформульовані вимоги до цілей системи менеджменту інформаційної безпеки.
– спрощено вимоги до текстового опису ризиків
– виключена обов'язковість випуску «Положення про прийняття остаточних ризиків» з боку вищого керівництва.
– встановлена чітка зв'язка «Положення про застосування - SoA».
– введено поняття і вимога щодо визначення «Власника ризику» замість «Власника активу».
– чітко сформульовані і доповнені вимоги з моніторингу СМІБ.

– спрощено вимоги до управління документацією та записами системи менеджменту інформаційної безпеки.

– чітко визначені вимоги з комунікацій в рамках системи менеджменту інформаційної безпеки [30].

Найбільш істотною зміною в основній частині є вимога щодо визначення «Власників ризиків».

Нові вимоги в рамках Програми «А» ISO / IEC 27001 до: 2013:

– A.6.1.4 Information security in project management
– A.12.6.2 Restrictions on software installation
– A.14.2.1 Secure development policy
– A.14.2.5 System development procedures
– A.14.2.6 Secure development environment
– A.14.2.8 System security testing
– A.15.1.1 Information security policy for supplier relationships
– A.15.1.3 Information and communication technology supply chain
– A.16.1.4 Assessment and decision of information security events
– A.17.1.2 Implementing information security continuity
– A.17.2.1 Availability of information processing facilities [31].

У додатку "А" кількість вимог (контролів) зменшилася з 133 до 113. Додаток «А» ISO / IEC 27001 містить перелік цілей і засобів управління, які збігаються з аналогічнимі цілями і засобами управління в ISO 27002, але не настільки деталізовані. Додаток «В» містить таблицю, в якій показано відповідність процедур СМІБ і етапів PDCA принципам Організації з економічного співробітництва та розвитку (OECD).

Якщо компанія вже впровадила ISO 9001 або ISO 14001, то їй знадобиться Додаток «С», який містить таблицю відповідності вимог стандартів ISO 9001, 14001 та 27001.

Організація може бути сертифікована акредитованими агентствами відповідно до цього стандарту. Процес сертифікації складається з трьох стадій:

Стадія 1 - вивчення аудитором ключових документів системи менеджменту інформаційної безпеки - положення про можливість застосування (SoA), план обробки ризиків (RTP), і ін. Може виконуватися як на території організації так і шляхом висилки цих документів зовнішньому аудитору;

Стадія 2 - детальний, глибокий аудит включаючи тестування впроваджених заходів та оцінка їх ефективності. Включає повне вивчення документів, які вимагає стандарт;

Стадія 3 - виконання інспекційного аудиту для підтвердження, що сертифікована організація відповідає заявленим вимогам. Виконується на періодичній основі [30].

Процедура сертифікації системи менеджменту за допомогою одного з міжнародних стандартів або їх комбінації підрозділяється на 4 етапи:

1 етап. Підготовка до сертифікації;

2 етап. Аудит 1-го ступеня (перевірка готовності до сертифікації);

3 етап. Аудит 2-го ступеня (сертифікаційний аудит);

4-ий етап. Видача сертифіката і нагляд.

1.2.3 Принципи ISO/IEC 27001

Стандарт ISO 27001 гармонізований зі стандартами систем менеджменту якості ISO 9001: 2000 та ISO 14001: 2004 та базується на їх основних принципах і процесний підхід.

Більш того, обов'язкові процедури стандарту ISO 9001 потрібні і стандартом ISO 27001. Структура документації за вимогами ISO 27001 аналогічна структурі за вимогами ISO 9001.

Велика частина документації, необхідна по ISO 27001, вже могла бути розроблена, і могла використовуватися в рамках ISO 9001.

Таким чином, якщо організація вже має систему менеджменту згідно, наприклад, з ISO 9001 або ISO 14001, то переважно забезпечувати виконання вимоги стандарту ISO 27001 в рамках вже існуючих систем [30].

Також основними принципами стандарту ISO 27001 є:

Конфіденційність інформації.

Цілісність інформації.

Доступність інформації.

Стандарт ISO 27001 зосереджений на захисті конфіденційності, збереження і доступності інформації в компанії. Це реалізується шляхом з'ясування потенційних проблем з інформацією (тобто оцінки ризиків), а потім визначення необхідних кроків для запобігання появи таких проблем (тобто зниження або обробки ризиків).

Тому основна філософія ISO 27001 базується на управлінні ризиками: з'ясувати, де знаходяться ризики, а потім систематично обробляти їх.

Існує чотири істотні переваги в бізнесі, які може отримати компанія при впровадженні цього стандарту інформаційної безпеки:

Відповідність правовим вимогам - з'являється все більше і більше законів, нормативних актів і договірних вимог, пов'язаних з інформаційною безпекою.

І гарною новиною є те, що багато з них можуть бути вирішені шляхом впровадження ISO 27001, оскільки цей стандарт надає компанії ідеальну методологію дотримання всіх нормативних актів.

Досягнення маркетингового переваги - якщо компанія пройшла сертифікацію, а конкуренти ні, то компанія можете отримати перевагу над конкурентами в очах клієнтів, які дуже обережно ставляться до питання безпеки їх інформації.

Зниження витрат - основна філософія ISO 27001 - запобігати появі інцидентів, пов'язаних з порушенням безпеки, тому що будь-який інцидент, великий чи маленький, коштує грошей.

Тому, запобігаючи їх, компанія заощадить досить багато грошей. І що найголовніше, інвестиції в ISO 27001 набагато менше очікуваної економії, яку компанія отримає.

Поліпшення організаційного процесу - у типових швидкозростаючих компаніяї немає часу призупинитися і визначити свої процеси і процедури.

Як наслідок, співробітники дуже часто просто не знають, що і коли необхідно робити і ким це повинно виконуватися.

Впровадження ISO 27001 допомагає вирішити такі ситуації, тому що це сприяє написанню компаніями своїх основних процесів (навіть тих, які не пов'язані з безпекою) і дозволяє скоротити втрату часу їх співробітниками [31].

Пов'язані стандарти з інформаційної безпеки та інші стандарти:

1. Стандарт ISO / IEC 27002 містить рекомендації щодо впровадження контролів, зазначених в ISO 27001.

Стандарт ISO 27001 вказує на 114 контролів, які можна використовувати, щоб знизити ризики для безпеки. ISO 27002 може бути вельми корисний, тому що він містить подробиці того, як впровадити ці контролі.

Стандарт ISO 27002, іменований раніше як ISO / IEC 17799, з'явився на основі Британського стандарту BS 7799-1 [32].

2. ISO / IEC 27004 містить рекомендації для оцінки інформаційної безпеки. Цей стандарт добре поєднується з ISO 27001, тому що пояснює, як визначити, чи досягла система менеджменту інформаційної безпеки своїх цілей [33].

3. ISO / IEC 27005 містить рекомендації для управління ризиками порушення інформаційної безпеки.

Це дуже гарне доповнення до стандарту ISO 27001, тому що містить деталі того, як здійснювати оцінку та обробку ризиків (а це, можливо, найскладніший етап впровадження). ISO 27005 з'явився на основі Британського стандарту BS 7799-3 [34].

4. ISO 22301 визначає вимоги до систем управління безперервністю бізнесу. Стандарт дуже добре поєднується з ISO 27001, тому що A.17 стандарту ISO 27001 вимагає впровадження безперервності бізнесу, але не надає занадто багато подробиць [35].

5. ISO 9001 визначає вимоги до систем менеджменту якості. І хоча, на перший погляд, у менеджменту якості і менеджменту інформаційної безпеки не так багато спільного, але, насправді, близько 25% вимог стандартів ISO 27001 та ISO 9001 аналогічні:

- управління документацією,
- внутрішній аудит,
- аналіз управління,
- коригувальні дії,
- постановка задач і управління компетенціями.

Це означає, що якщо компанія впровадила ISO 9001, то впровадити ISO 27001 буде набагато простіше [36].

Отже, ISO 27001 може бути впроваджений в будь-якій організації: комерційної або некомерційної, приватної або державної, маленької чи великої. Він був написаний провідними світовими експертами в області інформаційної безпеки і пропонує методологію для впровадження управління інформаційною безпекою на підприємстві.

1.3 Методи та засоби забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів

В рамках стандартів міжнародного (стандарти ISO) та національного рівнів (ДСТУ, НД ТЗІ) щодо інформаційної безпеки визначаються вимоги до захисту інформації, або її властивостей.

В англомовних стандартах, це класична модель CIA, щодо забезпечення вимог конфіденційності, цілісності та доступності інформації. Окремо виноситься вимога спостереженості (accountability).

Вимога конфіденційності висувається до інформації, всі інші – як до інформації так і до системи в цілому.

З метою цільового застосування (як механізму захисту так і попередження) стандартів ІБ в рамках даної моделі в ІТС також розглядаються три складові:

– апаратне забезпечення (hardware);
– програмне забезпечення (software);
– комунікаційна складова (communication), які представлено на рис. 1.5.

Відповідно до СІБ, захищеною, вважається ІТС, яка відповідає встановленим вимогам і гарантіям щодо забезпечення конфіденційності, цілісності, доступності та спостережності інформаційних активів.

Інформаційна безпека представляє собою проблему високої складності. Забезпечення інформаційної безпеки потребує комплексного підходу до розробки засобів захисту як на організаційному, так і на технічному рівні, тобто таке управління, що забезпечує механізм, який дозволяє реалізувати інформаційну безпеку.

Рис. 1.5. Модель інформаційної безпеки в ІТС

Управління інформаційною безпекою (англ. information security management) – частина загальної системи менеджменту (управління), метою

якого є забезпечення конфіденційності, цілісності та доступності інформаційних активів (документів, носіїв, додатків, інформаційних систем, знань персоналу тощо) [37].

Це безперервний процес реалізації політики безпеки підприємства на постійній основі, а також її постійного оновлення. Система управління інформаційною безпекою – СУІБ (англ. information security management system, ISMS) – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Міжнародна стандартизація складових системи управління інформаційною безпекою формує три напрямки розвитку в даній сфері: сімейство стандартів „Методи забезпечення безпеки" – ISO/IEC 27000-ISO/IEC 27037; сімейство стандартів „Методи та засоби забезпечення безпеки" – ISO/IEC 15408 („Загальні критерії", 3 частини), ISO/IEC 13335 (5 частин), ISO/IEC 18045; сімейство стандартів „Управління та аудиту інформаційних технологій" (CobIT, ITSM, ITIL та ін.) [38, 39, 40].

Серед зазначеного, окреме місце займає система міжнародних стандартів щодо управління ІБ – адже для установ, організацій, підприємств, які провадять діяльність в межах України достатньо впровадження КСЗІ та отримання Атестату відповідності вимогам нормативних документів системи технічного захисту інформації України.

Стандарти управління інформаційною безпекою – це модель системи менеджменту, яка визначає загальну організацію, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки.

У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої скорочення матеріальних втрат, зв'-

язаних з порушенням інформаційної безпеки, забезпечення не тільки надійного захисту інформації, але також організація ефективного доступу до даних та нормальна робота з ними [37].

Для установ, організацій, підприємств, які провадять діяльність на міжнародному рівні, важливою умовою підвищення ефективності цієї діяльності є наявність Сертифікату відповідності міжнародним стандартам серії ISO/IEC 27001 (оцінки і управління інформаційною безпекою) „Інформаційні технології – Засоби забезпечення безпеки", що ґрунтуються на авторитетних британських стандартах BS 17799 (з 2000 р. признаних міжнародними під назвою "International Standart ISO/IEC 17799. Information technology – Code of practice for information security management" [30].

Структура стандарту дозволяє вибрати ті засоби управління, які мають відношення до конкретної організації або сфери відповідальності всередині організації. У зв'язку з цим, виділяється ряд ключових елементів управління, що подаються як фундаментальні.

При цьому, поряд з елементами управління для комп'ютерів та комп'ютерних мереж, стандарт приділяє велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам.

Безумовно, що не всі пункти стандарту можливо застосовувати в умовах кожної організації, тому в стандарті реалізовано підхід, при якому його використовують як деяке "меню", з якого слід вибирати елементи, для конкретних умов. Цей вибір здійснюється на основі оцінки ризику та ретельно обґрунтовується [37].

Згідно ISO/IEC 27001: 2005 побудова ефективної системи УІБ можлива при реалізації напрямків А5-А15 (Додаток А ISO/IEC 27001: 2005) наведених в таблиці 1.1.

Таблиця 1.1

Напрямки побудови СУІБ згідно ISO/IEC 27000

<table>
<tr><td colspan="4">А.5 Політика в області безпеки</td></tr>
<tr><td colspan="4">А.6 Організація системи безпеки</td></tr>
<tr><td colspan="4">А.7 Класифікація активів та управління</td></tr>
<tr><td>А.8
Безпека та персонал</td><td>А.9
Фізична та зовнішня безпека</td><td>А.10
Менеджмент комп’ютерів та мереж</td><td rowspan="2">А.12
Придбання, розробка й обслуговування інформаційної системи</td></tr>
<tr><td colspan="3">А.11 Управління доступом до системи</td></tr>
<tr><td colspan="4">А.13 Менеджмент інцидентів інформаційної Безпеки</td></tr>
<tr><td colspan="4">А.14 Забезпечення безперервності бізнесу</td></tr>
<tr><td colspan="4">А.15 Відповідність законодавства</td></tr>
</table>

В залежності від конфіденційності інформації, яка зберігається, обробляється та передається в організації, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні організації, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови СУІБ.

Можливі наступні варіанти:

– досягнення необхідного рівня інформаційної безпеки за мінімальних затрат і допустимого рівня обмежень на технології зберігання, оброблення та передавання інформації у організації;

– досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технології зберігання, оброблення та передавання інформації у організації;

– досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технології зберігання, оброблення та передавання інформації у організації.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант [37].

Взагалі перелік стандартів серії ISO/IEC 27000 включає близько 20-ти найменувань – від стандарту ISO/IEC 27001 (Системи управління інформаційною безпекою) до стандарту ISO/IEC 27037 (Настанови з ідентифікації, виявлення, збору та збереження цифрових доказів).

Найбільш значимі з них, впровадження яких вже здійснюється або очікується найближчим часом, приведені в таблиці 1.2.

Таблиця 1.2

Перелік чинних та перспективних стандартів серії ISO/IEC 27000

Шифр стандарту	Найменування (призначення) стандарту
ISO/IEC 27000: 2009	Управління ІБ. Короткий огляд і словник
ISO/IEC 27001: 2005	Системи управління ІБ. Вимоги
ISO/IEC 27002: 2005	Звід практики для управління ІБ (*ISO/IEC 17799:2005*)
ISO/IEC 27003: 2010	Керівництво по реалізації системи управління ІБ
ISO/IEC 27004: 2009	Вимірювання в управлінні ІБ
ISO/IEC 27005: 2008	Ризик-менеджмент ІБ
ISO/IEC 27006: 2007	Вимоги до органів аудиту і сертифікації СУІБ
ISO/IEC 27007: 2011	Настанови щодо аудиту ІБ системи управління
ISO/IEC 27011: 2008	Настанови щодо управління ІБ для телекомунікацій
ISO/IEC 27031: 2011	Настанови щодо інформаційно-комунікаційних технологій. Готовність до безперервності бізнесу.

Названі стандарти отримали широке розповсюдження і послужили поштовхом для створення національних нормативних документів в галузі інформаційної безпеки в багатьох країнах світу.

В Україні, в 2012 р. презентовано державний стандарт ДСТУ ISO/IEC 27001:2010 „Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Система управління інформаційною безпекою. Вимоги”.

Також, в якості галузевих, з березня 2011 р. прийняті два стандарти Національного банку України:ДСТУ СУІБ 1.0/ISO/IEC 27001:2010 „Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги” (ISO/IEC 27001: 2005, MOD); ДСТУ СУІБ 2.0/ISO/IEC 27002:

2010 „Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою” (ISO/IEC 27002: 2005, MOD). [41, 42].

Слід зазначити, що застосування ДСТУ ISO/IEC 27001 для банківських структур є обов’язковим, для структур з іншими видами діяльності – на власний розсуд.

Окрім цього, для реалізації вимог СУІБ в Україні гармонізації потребують міжнародні стандарти ISO/IEC 27005: 2008 „Ризик-менеджмент ІБ” та ISO/IEC 27003:2010 „Керівництво по реалізації системи управління ІБ” [43, 44].

Перший надає структуру для визначення підходу до управління ризиками в залежності від області дії СУІБ, область застосування управління ризиками ІБ або сектора промисловості та процес оцінки інформаційних ризиків (ІР) (2 етапи): аналіз ІР (ідентифікація і кількісна оцінка активів, загроз, існуючих засобів контролю, вразливостей і наслідків; оцінювання ІР (управління ризиком на основі ітераційного підходу щодо його оцінки до отримання прийнятного значення).

Другий описує процес специфікації та проектування СУІБ з моменту початку проектування до подання планів впровадження системи [37].

Метою стандарту є надання практичної допомоги при реалізації СУІБ у межах організації відповідно до ISO/IEC 27001: 2005.

На основі стандарту ISO/IEC 27003: 2010 „Керівництво по реалізації системи управління ІБ” Департамент інформатизації Національного банку України розробив Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до галузевих стандартів Національного банку України з врахуванням особливостей банківської діяльності та вимог Національного банку України з питань ІБ.

1.4 Аналіз ризиків інформаційної безпеки

Походження терміну «ризик» бере свій початок з французької мови слова risqué або італійського risico і позначає можливість або ймовірність настання даної події з певними наслідками з кінцевими конкретними рішеннями або діями, де розглядається не тільки негативний тип ефекту, а й позитивний.

В СРСР ризик-менеджмент почав розвиватися після Другої світової війни і тільки в напрямку страхування, який вважався дорогим і неповним інструментом захисту від впливу ризику.

Початок по роботі з ризиками вважається стаття аспіранта Чиказького університету Гаррі Марковіца «Диверсифікація вкладень» («Portfolio Selection»), в якій була представлена математично обґрунтована стратегія диверсифікації інвестиційного портфеля, що допомагало грамотно розподілити вкладення і мінімізувати відхилення прибутковості від очікуваного показника.

В 1990 році Г.Марковіца була присуджена Нобелівська премія за те, що він вклав фундаментальні основи в розвитку і вивченні поняття ризику.

Спочатку робота з ризиками застосовувалася тільки до фінансової сфери, а ось вже в другій половині двадцятого століття з'явилися всі нині загальновідомі і приємним на даний момент методи визначення ризиків в різних областях науки. Хоча до цих пір багато підприємств спочатку не розробляють власну концепцію ризиків при «зародження» підприємства і тільки зіткнувшись з труднощами, приходять до цього [45, 46].

Так як суть будь-якого явища, процесу або об'єкта є діяльність, яка веде до формування результатів і розрізняються як: непрямі, прямі, конструктивні, деструктивні, псевдовипадкові, об'єктивні і суб'єктивні види результатів і т.д. тоді об'єктивний результат є наслідком певного виконання процесу, який безпосередньо пов'язаний з його суттю, а суб'єктивний результат є виконання процесу з недостатнім рівнем визначеності і повноти інформації. переважна кількість існуючих ризиків зустрічаються на практиці пов'язано саме з суб'єктивними результатами здійснення і виконання процесу.

Тому можна сказати, що практично всі ризики є суб'єктивний результат виконання процесу, і вони мають недолік як кількісної, так і якісної інформації про певний даному процесі.

На даному етапі розвитку галузі ризиків в інформаційних технологіях існує безліч типізації ризиків. Інформаційні ризики, які виникають в розглянутих процесах і проектах, відрізняються між собою, як за сукупністю внутрішніх і зовнішніх факторів, так і за часом і місцем їх виникнення.

На даний момент ще не склалося однозначного поняття про те, що ж із себе представляє інформаційний ризик. Деякі фахівці розглядають інформаційний ризик як подію, яка безпосередньо впливає на інформацію: її видалення, спотворення, порушення її конфіденційності або доступності [47].

Ризики поділяються за характером на зовнішні і внутрішні; за часом виникнення на минулі або ретроспективні і майбутні або перспективні; за фактором виникнення такі, як проектні, операційні ризики, процесні, організаційні; за наслідками на чисті і спекулятивні.

При цьому вони впливають на їх рівень, на спосіб аналізу і методи первинного та подальшого опису. Оскільки всі види ризиків взаємопов'язані, отже, вони впливають на здійснювану діяльність, як по окремо, так і в сукупності між собою. Необхідно класифікувати безліч ризиків за критеріями і ознаками, за допомогою яких їх можна об'єднати в загальні поняття, такі як: характер, час і чинники виникнення, наслідки і т.д. [46].

У свою чергу ризики за характером поділяються на зовнішні і внутрішні; по часу виникнення на минулі або ретроспективні і майбутні або перспективні; по фактору виникнення такі, як проектні, операційні ризики, процесні, організаційні; по наслідкам на чисті і спекулятивні.

Так само виділяється класифікація ризиків за ступенем наслідків виникнення та складається з: допустимого ризику, критичного ризику і катастрофічного ризику. Ця класифікації є важливою при прийнятті рішень щодо здійснення будь-якої діяльності, пов'язаної з ризиками.

Сутність будь-якого підходу до управління ризиками полягає в аналізі чинників ризику і прийнятті адекватних рішень по обробці ризиків [48].

Важливим етапом є ідентифікація ризику - це одна зі стадій аналізу ризиків що дозволяє виявити, оцінити і зрозуміти причини, які ведуть до появи ризику і яку необхідно проводити перед здійсненням класифікації ризиків. Від правильності її проведення і буде залежати результат обраного методу для усунення шкоди.

Фактори ризику - це ті основні параметри, якими оперують при оцінці ризиків, а саме:

– Актив (Asset).
– Загроза (Threat).
– Збиток (Loss).
– Уразливість (Vulnerability).
– Повернення інвестицій (ROI).
– Механізм контролю (Control).
– Розмір середньорічних втрат (ALE).

Способи аналізу та оцінки цих параметрів визначаються використовуваної в організації методологією оцінки ризиків [49].

Інформаційний ризик є небезпечним для об'єкта або суб'єкта інформатизації подією, при реалізації якого можливо завдати шкоди, як для інформаційної сфери, так і для інформаційного обслуговується об'єкта в цілому. Інформаційні ризики пов'язані з інформаційною безпекою (ІБ) за допомогою сучасних методик аналізу і управління ризиками.

Визначення ризиків в сфері ІБ - це ймовірність того, що підприємство або організація можуть зазнати збитків через порушення безпеки інформаційної системи (ІС).

При цьому часто поняття ризику розглядається з поняттям загрози, де загроза ІБ - це потенційно можлива подія, яке може бути здійснено навмисно

або випадково, але при цьому надає небажаний вплив як на комп'ютерну систему, так і на інформацію, яка знаходиться і обробляється в ній.

Основна відмінність ризику від загрози полягає в тому, що ризик має як кількісну оцінку можливих втрат, так і оцінку ймовірності реалізації загрози [45].

Інформаційний ризик є небезпечне для об'єкта або суб'єкта інформатизації подія, при реалізації якої можливо завдати шкоди, як для інформаційної сфери, так і для інформаційного обслуговується об'єкта в цілому.

Якщо розглядати забезпечення ІБ до ІС для будь-яких проектів вимагають фінансових витрат на їх реалізацію необхідно чітко сформулювати завдання і поставити конкретну мету яку необхідно досягти.

Існують різні способи обґрунтувань проектів підсистем забезпечення безпеки, але на практиці свою реалізацію отримали в основному два підходи: перший полягає в перевірці відповідності рівня захищеності ІС вимогам стандартів в даній області, другий - в побудові системи забезпечення ІБ, яка виробляє як оцінку, так і управління ризиками.

Для того, щоб ризик описувати, необхідно визначити актив (ресурс) - це елемент ІС, який має цінність і підлягає захисту, і тоді ризики можна ідентифікувати за загрозою (з допомогою якої викликаний даний ризик), ресурсу (для якого реалізована дана загроза) і уразливості (завдяки якій може бути реалізована дана загроза щодо даного ресурсу).

Тобто при оцінці ризику, обов'язково необхідно оцінити: як часто відбувається небажана подія, яка ймовірність даного ресурсу завдати шкоди, а також, скільки буде складати втрати від завданих збитків [45].

Проведення оцінки ризиків є дуже тривалою і трудомісткою задачею, при цьому немає стандартних загальноприйнятих підходів і методик для оцінки ризиків в конкретній ситуації. В основному фактори ризику, такі як загроза, вразливість, збиток розглядаються і аналізуються за допомогою еврис-

тичних підходів і методів за рахунок проведення експертизи різними експертами, за рахунок цього результати можуть відрізнятися один від одного [50] і при цьому можуть виникати такі проблеми:

- інформація про ризик дуже часто не повна і має неоднозначні властивості;

- для досягнення поліпшення оцінок необхідно призначати не менше двох фахівців в даній області;

- існує певна складність побудови моделі ІС і оцінки її уразливості;

- складність об'єднати елементи в одну систему з різних джерел;

- потрібен тривалий час на оцінку ризиків, при цьому втрата актуальності результатів настає дуже швидко.

Тобто необхідно перебрати безліч методів оцінки ризику ІБ, який буде забезпечувати найкращий результат з максимальною вірогідністю оцінки [51].

Зараз на практиці застосовується безліч різноманітних методик для аналізу інформаційних ризиків. Відмінність існуючих методик полягає в тому, як вони оцінюються: кількісно, якісно або за допомогою шкал оцінки рівня ризику. Розглянемо дані методики.

Для оцінки рівня ризику організаціями використовується шкали оцінки, які в більшій мірі несуть в собі описовий характер і діляться на: від 0 до 1 і розбивки на рівні: «дуже низький», «низький», «середній», «високий», «дуже високий» [52].

Таблиця 1.3

Рівні шкали для оцінки факторів ризику

Рівні шкали		Загрози	Збитки	Вразливість (В)
Дуже низький	0-0.2	Подія практично ніколи не відбувається	Незначні втрати матеріальних засобів і ресурсів	В, якою можна Знехтувати
Низький	0.2-0.4	Подія трапляється рідко	Більш помітні втрати матеріальних активів	Незначна В, яку можна легко усунути

Середній	0.4-0.6	Подія цілком можливо при певному збігу обставин	Достатні втрати матеріальних активів або ресурсів	Помірна В
Високий	0.6-0.8	Швидше за все, подія відбудеться при організації атаки	Значної шкоди репутації та інтересам, що може становити загрозу для продовження діяльності	Серйозна В, Ліквідація можлива, але пов'язана зі значними Витратами
Дуже високий	0.8-1	Подія, найімовірніше, відбудеться при організації атаки	Руйнівні наслідки і неможливість ведення діяльності	Критична в, мала частка можливості її усунення

Кожна організація розробляє шкалу оцінювання самостійно, тому можуть зустрічатися різні градації у вигляді присвоєння даних наслідків цифрових значень, які можуть бути як лінійними, так і нелінійними, при цьому сенс оцінки залишається колишнім.

Якщо необхідно отримати комбінації ймовірності і впливів, то використовуючи шкалу рівнів впливу, будується матриця ймовірностей, яка дає можливість присвоєння рангу ризиків: низький, середній або високий [53].

Кількісний метод - включає в себе кількісну оцінку ризиків, яка використовується для досліджуваних загроз. При цьому пов'язані з ними ризики можна буде зіставити з кінцевими кількісними значеннями (в грошовому еквіваленті, в людських ресурсах або відсотках і т.д.) і дозволить отримати результат у вигляді конкретних значень об'єктів оцінки ризику при реалізації загроз ІБ [54].

При кількісному аналізі ризику використовуються різні методи оцінки: аналітичний метод; метод аналізу доцільності витрат; метод експертних оцінок; статистичний метод; метод використання аналогів.

Кількісна оцінка ризиків проводитися за допомогою різних чинників:

– необхідно визначити цінність інформаційного активу;

– провести кількісну оцінку потенційного збитку від реалізації кожної загрози для кожного розглянутого інформаційного активу;

– визначити ймовірність реалізації кожної із загроз ІБ;

– визначити потенційний збиток для кожної загрози і активу за певний встановлений період часу.

Далі для кожної загрози провести отриманий аналіз збитку. Після проведення кількісної оцінки приймається рішення, що робити з ризиком: прийняти, знизити або перенести [55].

Якісний метод не використовує в своїй оцінці грошових вимірів, а використовується привласнення показника за шкалами (п'ятибальна шкала від 0 до 5 або десятибальна від 0 до 10 або трибальна: низька, середня, висока).

Даний метод проводиться співробітниками (компетентними в області проведення оцінки ризиків та загроз) за допомогою різних методів: анкетування, тренінги, особисті зустрічі, групові зустрічі, опитування, інтерв'ювання та після збору інформації вже проводитися якісна оцінка ризиків, в якій необхідно визначити:

- цінність інформаційних активів;

- ймовірність реалізації загрози для інформаційного активу;

- можливість досягнення позитивного результату реалізації загрози в залежності від даного стану ІБ і впроваджених засобів захисту і заходів;

- по кожній загрозу провести аналіз кінцевих результатів і рівень ризику.

Кінцевим результатом проведення якісної оцінки повинен бути конкретний результат для зниження ризиків до мінімального або прийнятного рівня, а також складено список заходів безпеки і певний набір правил і дій [56].

Розглянувши методи аналізу інформаційних ризиків можна зробити висновок, що за допомогою всіх методів можна визначити перелік актуальних загроз, вибрати ефективні контрзаходи і засоби захисту.

Головне визначитися, що треба отримати в результаті - оцінку в грошовому еквіваленті і витратити на це більше часу, але отримати конкретні цифри

щодо витрат і можливого збитку, використавши кількісний метод оцінки ризиків.

Або вибрати більш простий і швидкий шлях - отримавши суб'єктивний відповідь на витрати і вигоди від впровадження засобів захисту інформації та збитки, використавши якісний метод або метод шкали оцінки рівня ризику [53].

Отже, управління ІБ все більшою мірою ставати не тільки необхідним, але і обов'язковим елементом у функціонуванні та управлінні будь-якого підприємства, організації.

При цьому ІБ має значення не тільки для збору, обробки та зберігання інформації, а й для контролю: своєчасного виявлення загроз ІБ, вразливостей інформаційної системи і заходи щодо їх усунення та попередження, використовуючи існуючі методи оцінки рівнів ризиків і впровадження нових, використавши основні закони міжнародних стандартів управління ІБ.

Висновок до розділу I

Інформаційна безпека - практика запобігання несанкціонованому доступу, використання, розкриття, спотворення, зміни, дослідження, записи або знищення інформації.

Це універсальне поняття застосовується незалежно від форми, яку можуть приймати дані (електронна або, наприклад, фізична). Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації.

ISO / IEC 27001 - міжнародний стандарт по інформаційної безпеки, розроблений спільно Міжнародною організацією зі стандартизації та Міжнародної електротехнічної комісією.

ISO 27001 може бути впроваджений в будь-якій організації: комерційної або некомерційної, приватної або державної, маленької чи великої. Він

був написаний провідними світовими експертами в області інформаційної безпеки і пропонує методологію для впровадження управління інформаційною безпекою на підприємстві.

Він також дозволяє компаніям отримати сертифікацію, що означає, що незалежний орган із сертифікації підтвердить, що організація впровадила інформаційну безпеку відповідно до стандарту ISO 27001.

В рамках стандартів міжнародного (стандарти ISO) та національного рівнів (ДСТУ, НД ТЗІ) щодо інформаційної безпеки визначаються вимоги до захисту інформації, або її властивостей.

При аналізі ризиків ІБ можна виділити недоліки: оцінка носить практично завжди формальний характер; оцінюється без розслідування на випадкової, а не постійній основі. Це впливає на те, що існуючі важливі дані залишаються неврахованими і обізнаність осіб, які приймають, якесь рішення по ліквідації ризиків у багатьох організаціях буде недостатньою. Необхідно так само пам'ятати, що головний ризик - це людина, яка надає для ІБ найбільшу небезпеку в навмисній або не навмисній помилці.

Так як відсутні загальноприйняті підходи і методики для оцінки ризиків і в кожному конкретному випадку необхідно ретельно прораховувати і продумувати всі фактори ризику, проводити аналіз і розрахунок, що є дуже трудомістким завданням, крім того ще й існує ймовірність отримати помилковий результат.

З усіх методів оцінки ризиків необхідно застосовувати сукупність методів аналізу, обробки інформації та тільки після цього оцінювати ризики ІБ, і здійснювати управління ІБ. Так само необхідно зменшувати «ручну працю», використовувати існуючі сучасні методології оцінки ризиків, і все більше переходити до оцінки ризиків за допомогою інтелектуального аналізу даних нейронних мереж.

РОЗДІЛ ІІ. ХАРАКТЕРИСТИКА ПІДПРИЄМСТВА

2.1. Характеристика підприємства

Об'єктом дослідження в дипломній роботі є ТОВ "КБ "ХОРТ".

Повне найменування юридичної особи - ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ КОНСТРУКТОРСЬКЕ БЮРО ХОРТ.

Код ЄДРПОУ – 40336546.

Дата реєстрації - 11.03.2016 (4 роки 8 місяців).

Розмір статутного капіталу - 10 000,00 грн.

Організаційно-правова форма - товариство з обмеженою відповідальністю.

Форма власності - недержавна власність.

Адреса: м.Київ, Подільський район, провулок Хоревий, будинок 1.

Види діяльності:

Основний:

– Діяльність у сфері оборони.

Інші:

– Виробництво електричного й електронного устаткування для автотранспортних засобів.

– Виробництво військових транспортних засобів.

– Виробництво зброї та боєприпасів.

– Оброблення металів та нанесення покриття на метали.

– Механічне оброблення металевих виробів.

– Виробництво інших готових металевих виробів, н. в. і. у.

– Виробництво електронних компонентів.

– Виробництво обладнання зв'язку.

– Виробництво інструментів і обладнання для вимірювання, дослідження та навігації.

– Діяльність приватних охоронних служб.

– Діяльність у сфері охорони громадського порядку та безпеки.

– Діяльність у сфері безпроводового електрозв'язку.

– Діяльність у сфері супутникового електрозв'язку.

– Інша діяльність у сфері електрозв'язку.

– Діяльність у сфері інжинірингу, геології та геодезії, надання послуг технічного консультування в цих сферах.

– Технічні випробування та дослідження.

– Спеціалізована діяльність із дизайну.

– Ремонт і технічне обслуговування готових металевих виробів.

– Ремонт і технічне обслуговування електронного й оптичного устаткування [57].

ТОВ "КБ "ХОРТ" займає 7 поверхів великого будинку, де прокладати кабель економічно не вигідно і проблематично. Схема розташування об'єктів на території підприємства представлена на малюнку 2.1.

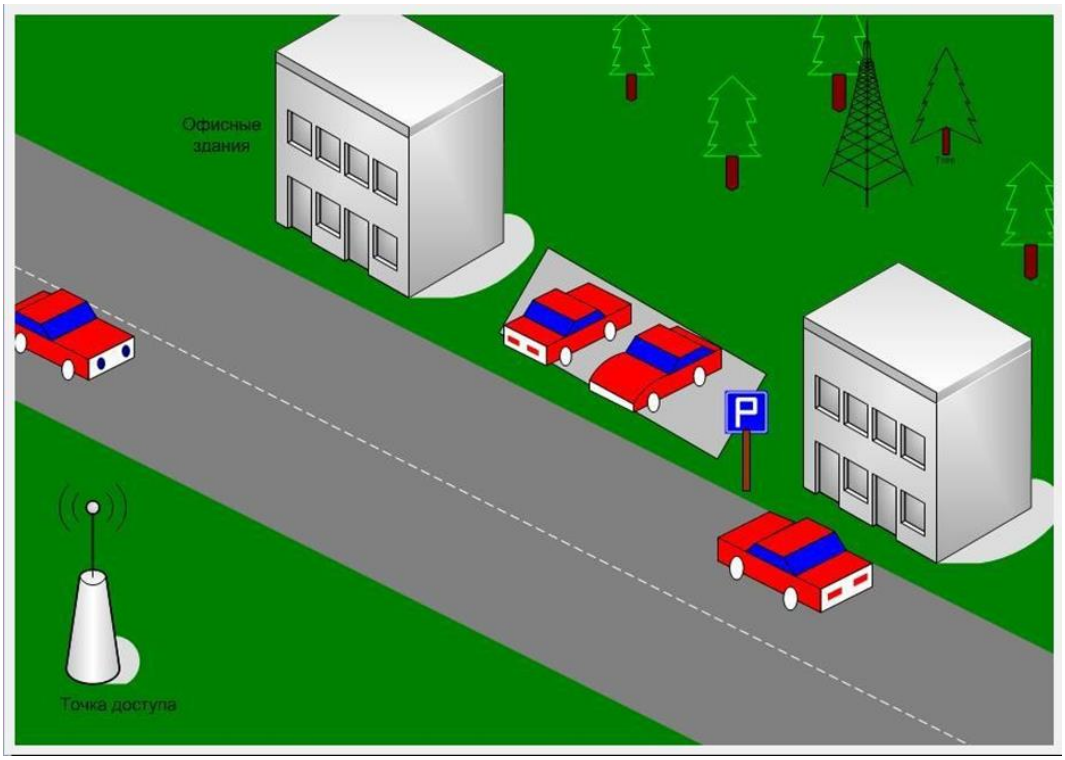

Рис. 2.1 - Схема розташування об'єктів ТОВ "КБ "ХОРТ"

Підприємство займає споруду площею близько 50 000 квадратних метрів і висотою в 7 поверхів.

На першому поверсі будівлі знаходиться кафетерій з інтернет доступом. Всі інші поверхи є службовими.

Чисельність комп'ютерів, ноутбуків, планшетів в службових приміщеннях близько 600 шт.

Територія, на якій розташоване підприємство, дуже велика, в рамках території також виникає необхідність забезпечення доступу мобільних пристроїв до єдиної мережі, а також забезпечення працездатності.

2.2. Аналіз діючої інформаційної системи

Інформаційна система підприємства ТОВ "КБ "ХОРТ" є взаємопов'язаною сукупнісю засобів, методів і персоналу, які використовуються для зберігання, обробки, і видачі інформації в інтересах досягнення поставленої мети.

У кожного фахівця в компанії є своє робоче місце, яке обладнане комп’ютером.

Крім того в компанії є багатофункціональні пристрої. На комп'ютери встановлений комплект програмного забезпечення. Склад типового робочого місця фахівця представлений в таблиці 2.1.

Таблиця 2.1

Склад робочого місця фахівця ТОВ "КБ "ХОРТ"

Назва підсистеми	Назва компоненту	Кількість
Процесор	Intel Core i7 950 3067MHz,8Mb, LGA1366	1
Системна плата	ASUS P6T Deluxe V2, Intel X58	1
Оперативна пам’ять	6Gb (3*2Gb) DDR3 1600Mhz Corsair XMS3	1
Накопичувачі HDD	500Gb Western DigitalSATA-II 16mb	1
Відеокарта	640Mb NVIDIA GeForce GTX 470	1

Корпус без блоку живлення	MiditowerGigaByte GZ-KX9 Black ATX безБП	1
Маніпулятор	Defender Pluto 310 B, USB+PS⁄2	1
Блок живлення	Corsair CMPSU-850TX 850W	1
Клавіатура	KBS-8	1
Відеомонітор	16" MONITOR ASUS VH232T BK	2

ТОВ "КБ "ХОРТ" займає 7 поверхів однієї будівлі. Комп'ютери підприємства не включені в єдину локальну мережу. Мережа організована тільки в рамках другого і третього поверху.

Для організації мережі цього сегмента використовується топологія «зірка», причому в кожному кабінеті, де більше одного комп'ютера, є концентратор, що з'єднує комп'ютери всередині кабінету.

Всі концентратори на цих поверхах підключаються до концентратора, що знаходиться в кабінеті у техніків. Таким чином, в компанії використовується мережа «ієрархічна зірка».

Всі комп'ютери володіють однаковими характеристиками. Комп'ютери в мережі мають стандартну мережеву карту з роз'ємом RJ45 і мережеву операційну систему.

В кожному кабінеті розташовані концентратори SuperStack II Hub 100 Base T4 виробництва 3Com Corp.

Комп'ютери третього поверху підключаються до концентратора, що знаходиться в кабінеті у техніків на другому поверсі.

На підприємстві використовуються різні за властивостями і функцій програмні продукти.

Програмне забезпечення ТОВ "КБ "ХОРТ" включає сукупність програм для реалізації цілей і завдань інформаційної системи, пов'язаних з основною діяльністю компанії, а також нормального функціонування комплексу технічних засобів.

Системне програмне забезпечення комп'ютерів представлено в таблиці 2.2.

Таблиця 2.2

Основне системне програмне забезпечення ТОВ "КБ "ХОРТ"

Найменування	Кількість
ОС Windows 7 Корпоративна	48
Антивірус ESET Antivirus	48
Архіватор 7Zip	48

Широко застосовуються архіватори Rar, WinZip, WinRar. Всіма працівниками використовується текстовий редактор MicrosoftWord. В процесі роботи, співробітники стикаються з необхідністю детального аналізу і моніторингу всіляких даних.

Тому застосування знаходить табличний процесор Microsoft Excel, який дозволяє реалізувати найбільш «популярні» методи обробки результатів соціологічних досліджень.

Також на підприємстві є програмний продукт 1С: «Бухгалтерія», який є типовим рішенням для автоматизації бухгалтерського і податкового обліку, включаючи підготовку обов'язкової звітності.

Конфігурація «Бухгалтерія» підприємства дозволяє реалізувати будь-яку схему обліку і може використовуватися як автономно, так і спільно з іншими компонентами.

На рис .2.1 приведена архітектура мережі підприємства ТОВ "КБ "ХОРТ" (2 і 3 поверх).

Варто відзначити, що на малюнку наведені тільки приміщення першого, другого і третього поверхів. Це пов'язано з тим, що на інших чотирьох поверхах комп'ютери не підключені до єдиної локальної провідної мережі.

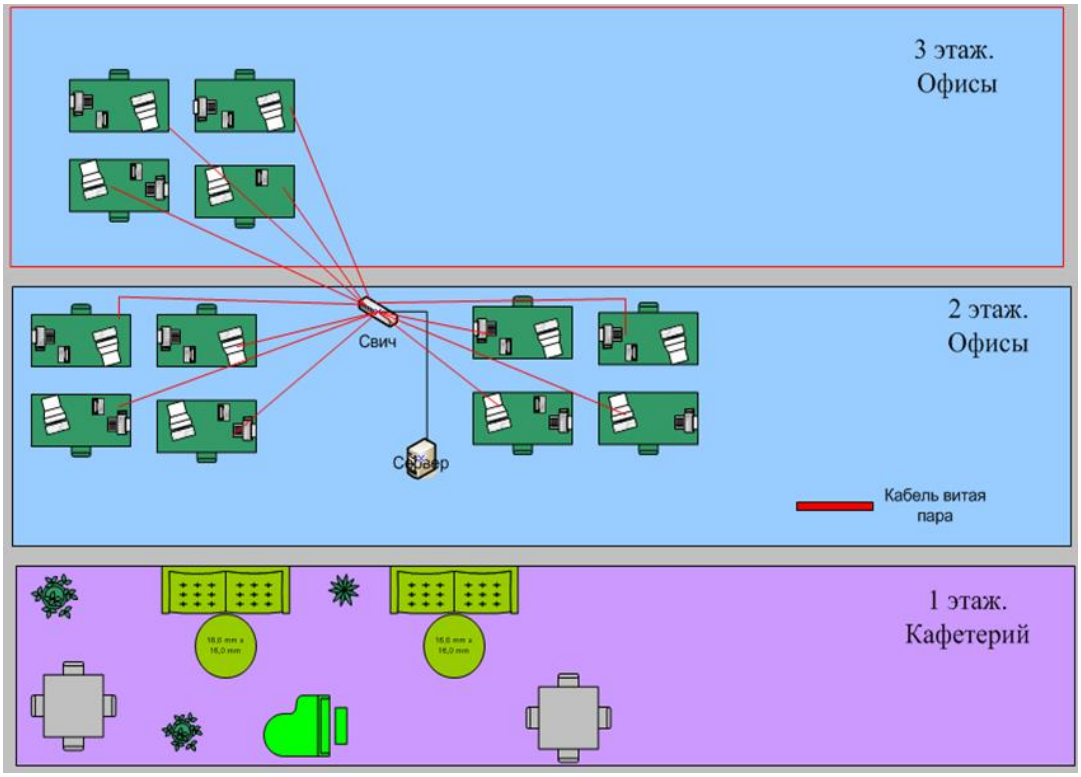

Рис. 2.2. Архітектура локальної мережі ТОВ "КБ "ХОРТ" (2 і 3 поверх).

На верхніх поверхах комп'ютери підключаються до мережі на основі технології WiMAX. Схема мережі представлена на малюнку 2.3.

Для організації мережі на основі WiMAX було виконано наступне:

- укладено договір з постачальником послуг;

- встановлено пристрій WiMAX роутер, який забезпечить підключення всіх пристроїв до єдиної мережі;

- на кожен пристрій встановлені адаптери, організовані точки доступу;

- встановлено параболічні антени для посилення сигналів точок доступу, віддалених комп'ютерів;

- всі пристрої, що знаходяться в будівлі, підключені до роутера (маршрутизатора);

- налаштована мережа Інтернет, локальна мережа, принт-сервер.

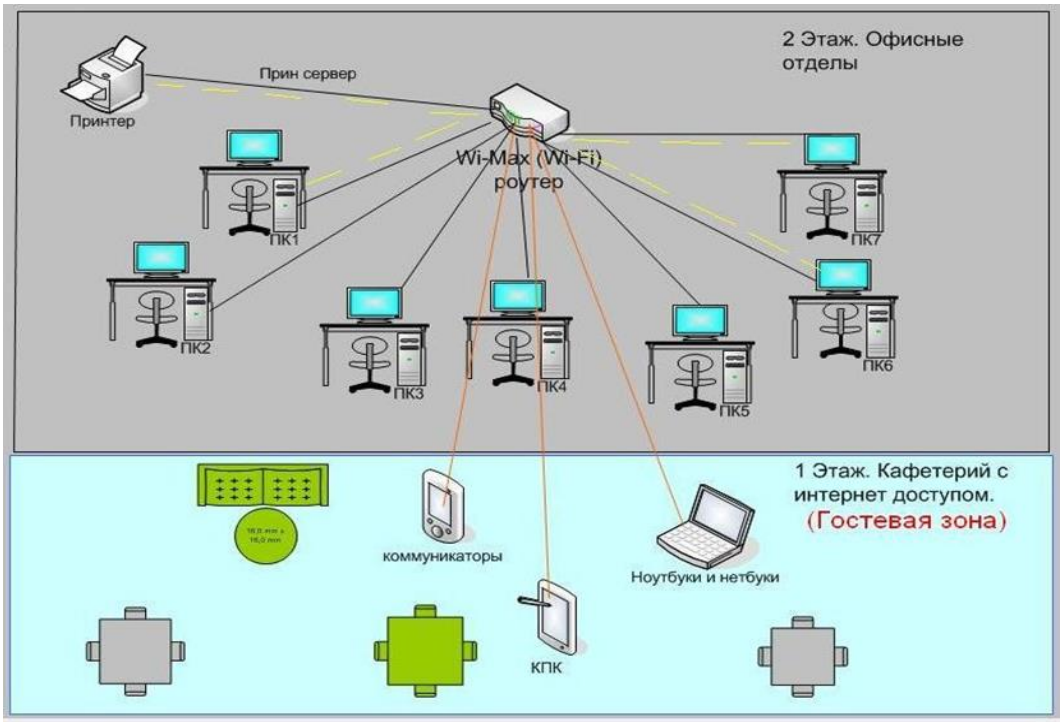

Рис. 2.3. Архітектура локальної мережі WiMax

Для того, щоб можна було використовувати локальну мережу і Принт-сервер, був обраний гібридний роутер, модель яка дозволить працювати в мережах WiMax та Wi-fi. Цей роутер повинен поширювати Інтернет між усіма комп'ютерами за технологією WiMax, а для організації локальної мережі і принт-сервера буде використовуватися технологія Wi-fi.

Так як приміщення на 1 поверсі займає кафетерій, то необхідно забезпечити загальний доступ на використання інтернету для комп'ютерів кафетерію, але обмежити їх доступ в локальну мережу.

Всіх відвідувачів кафе зі своїми пристроями, які оснащені модулями WiMax та бажають скористатися послугою Інтернет, потрібно поміщати в гостьову зону, яка буде обмежувати їх, надаючи їм певну швидкість і запитуючи пароль доступу до системи, який вони будуть отримувати тільки при замовленні.

Для підключення пристроїв до єдиної мережі на основі WiMAX були придбані адаптери і точки доступу. Для організації мережі було придбано обладнання (таблиця 2.3).

Таблиця 2.3

Перелік обладнання для організації мережі

Назва	Кількість	Дальність, м	Призначення
Безпровідний USB адаптер 802.11g, до 108 Мбіт/с dwa-120	30	100	Встановлюється в комп'ютер для зв'язку з бездротовими мережами
AirPremier N зовнішня дводіапазона безпровідна 2,4 ГГц (802.11b/g/n)/ 5 ГГц (802.11a/n) точка доступа з підтриманням PoE, до 300 Мбіт/с DAP-3520	2	100	Точка доступу Wi-Fi для зв'язку між комп'ютерами внутрішньої мережі
RangeBooster N безпровідний 2,4 ГГц (802.11n) USB-адаптер, до 300 Мбіт/с dwa-120	1	100	Передача великих обсягів інформації

Роутер (або маршрутизатор) - пристрій, що служить забезпеченню багатьох функцій, таких як: колективний доступ в Інтернет, IP-телефонія і побудова локальних мереж LAN. Саме роутер забезпечує підключення всіх пристроїв до єдиної мережі і організації трафіку між ними. Для організації мережі знадобиться роутер (таблиця 2.4).

Таблиця 2.4

Перелік обладнання для організації мережі

Назва	Кількість	Дальність, м	Призначення
Роутер ASuS WL 500WWiMAXWifi до 20 mbit	1	100	Доступ в Інтернет. перетворення сигналу в Wi-fi

При використанні даного роутера, швидкість інтернетсоединенняWiMAXсоставляет до 20 Мбіт / сек. Цей маршрутизатор, підтримує 802.11n - багатофункціональний: він сумісний так само і з 802.11b / g, тому може використовуватися при передачі мультимедіа потоків.

Проектована мережа повинна забезпечувати хороший рівень сигналу. Однак у зв'язку з тим, що мережа охоплює великі відстані, сигнали при передачі можуть послаблюватися. Для посилення сигналу точок доступу необхідно використовувати параболічні антени (таблиця 2.5).

Таблиця 2.5

Перелік обладнання для організації мережі

Назва	Кількість	Дальність, м	Призначення
Параболічна антена з високим коефіцієнтом посилення, 21 dBi ANT24-1800	4	100	Посилення сигналу точок доступу і віддалених комп'ютерів

DLink ANT24-2100 підключається до безпровідних пристроїв DLink стандартів 802.11b і 802.11g (2.4 ГГц) і має коефіцієнт посилення 21 dBi.

Пасивна антена також може бути підключена до бездротового обладнанню 802.11b і 802.11g інших виробників. D-Link ANT24- 2100 надає можливість суттєво розширити площу покриття існуючої бездротової мережі і / або створити бездротової міст для передачі даних на великі відстані.

На підприємстві використовується система відеоспостереження для захисту конфіденційної інформації. Варто відзначити, що система відеоспостереження включає камери в коридорах, біля входів, але не передбачає відеоспостереження в кабінетах. У зв'язку з тим, що необхідно забезпечити захист цілісності і конфіденційності документів, з якими співробітники працюють в кабінетах, необхідно забезпечити відеоспостереження всередині робочих кабінетів. Оскільки є 47 кабінетів, то потрібно встановити додатково 47 камер відеоспостереження.

2.3. Організаційні заходи забезпечення інформаційної безпеки і захисту інформації підприємства

Активи (ресурси) - це все, що має цінність або знаходить корисне застосування для організації, її ділових операцій і забезпечення їх безперервності. Належне управління та облік активів повинні бути однією з основних обов'язків керівників усіх рівнів [58].

До основних активів належать інформація, інфраструктура, персонал. Без інвентаризації активів на рівні службової діяльності неможливо відповісти на питання, що саме потрібно захищати.

Були виявлені наступні потоки інформації:

- особисті справи працівників;
- інформація про бойову техніку;
- дані про споруди та матеріальне забезпечення підприємства;
- дані за наказами, розпорядженнями підприємства;
- бухгалтерська та управлінська звітність.

Результат ранжирування активів являє собою інтегровану оцінку ступеня важливості активу для підприємства, взяту за п'ятибальною шкалою і представлену в таблиці 2.6.

Таблиця 2.6

Результати ранжування активів

Назва активу	Цінність активу (ранг)
Програмне забезпечення	10
Працівники	11
Комп'ютерні засоби	9
Інформаційні послуги	3
Текстові повідомлення	12
Внутрішня переписка	8
Дані про споруди та матеріальне забезпечення підприємства	1
Видаткові накладні	6

Дані за наказами, розпорядженнями, заходами, розпорядку підприємства	3
Інвентаризаційна відомість	4
Прибуткові накладні	5
Бухгалтерська та податкова звітність	7

Оцінка загроз активів проведена на підставі вимог стандарту ISO / IEC TO 13335-3-2007 .

Активи, що мають цінність і характеризуються певною ступенем уразливості, щоразу наражаються на ризик в присутності загроз. Завдання аналізу ризику полягає у визначенні та оцінці ризиків, яким піддається система інформаційних технологій і її активи, з метою визначення та вибору доцільних і економічно обґрунтованих засобів забезпечення безпеки.

Для оцінки ризиків обраний метод, який пропонує використання таблиці «штрафних балів» для кожної комбінації цінності активів, рівня загроз і вразливостей.

Для кожного активу розглядають вразливі місця і відповідні їм загрози. Якщо є вразливі місця без відповідної загрози або загрози без відповідного уразливого місця, то вважають, що в даний час ризик відсутній.

Потім ідентифікують відповідний ряд матриці по цінності активу, а відповідну колонку - за ступенем загрози і вразливості. Цінність справжнього методу полягає в ранжируванні відповідних ризиків (таблиця 2.7).

Таблиця 2.7

Результати оцінки ризиків інформаційних активів організації

Ризик	Актив	Ранг ризику
Втрата цілісності	Дані за наказами, розпорядженнями, заходами, розпорядку підприємства	9
Втрата цілісності	Інформаційні послуги	9
Втрата конфіденційності	Внутрішня переписка	8

Втрата конфіденційності	Прибуткові накладні	8
Втрата конфіденційності	Видаткові накладні	7
Втрата конфіденційності	Інвентаризаційна відомість	6
Порушення цілісності	Програмне забезпечення	4
Втрата доступності	Дані про споруди та матеріальне забезпечення підприємства	4
Втрата доступності	Бухгалтерська та податкова звіт-ність	1

Дана таблиця містить ризики по найбільш цінних інформаційних активів, ранжирування в порядку убування.

Результати оцінки ризиків є підставою для вибору і формулювання завдань щодо забезпечення інформаційної безпеки підприємства, і вибору захисних заходів.

Таким чином, на основі аналізу можна виявити такі основні проблеми:

1. Відсутність антивірусного ПО на самих АРМ.
2. Застаріле антивірусне ПЗ на сервері.
3. Відсутність системи контролю доступу службовців до чужих АРМ.
4. Відсутність системи відеоспостереження в кабінетах.
5. Відсутність політики паролів.

Всі ці проблеми повинні враховуватися при плануванні комплексної системи захисту в ТОВ "КБ "ХОРТ".

Завдання щодо захисту інформації покладено на співробітників технічного відділу частині, а також на керівників підрозділів.

Результати оцінки діючої системи безпеки інформації, відображають, наскільки повно виконуються однотипні об'єктивні функції при вирішенні завдань забезпечення захисту інформації (таблиця 2.8).

Таблиця 2.8

Аналіз виконання завдань із забезпечення інформаційної безпеки

Основні завдання щодо забезпечення інформаційної безпеки	Ступінь виконання
забезпечення безпеки процесу управління підприємством, захист інформації та відомостей, що є комерційною таємницею	Середній
організація роботи з правового, організаційного та інженерно-технічного захисту комерційної таємниці	Середній
організація спеціального діловодства, виключає несанкціоноване отримання відомостей, що є комерційною таємницею	Середній
запобігання необґрунтованому допуску та відкритого доступу до відомостей і робіт, що становлять комерційну таємницю	Низький
виявлення і локалізація можливих каналів витоку конфіденційної інформації в процесі повсякденної виробничої діяльності та в екстремальних (Аварія, пожежа тощо.) Ситуаціях	Середній
забезпечення режиму безпеки при здійсненні таких видів діяльності, як різні зустрічі, переговори, наради, засідання та інші заходи, пов'язані з діловою співпрацею на національному та міжнародному рівні	Високий
забезпечення охорони території, будівель приміщень, з захищається	Високий

В першу чергу необхідно звернути увагу на ті аспекти захисту інформації, які характеризуються низьким і середнім ступенем виконання. Крім того, важливо забезпечити комплексний характер захисту.

Висновок до розділу II

Об'єктом дослідження в дипломній роботі є ТОВ "КБ "ХОРТ". Основна форма діяльності – діяльність у сфері оборони.

Підприємство займає споруду площею близько 50 000 квадратних метрів і висотою в 7 поверхів. На першому поверсі будівлі знаходиться кафетерій з інтернет доступом. Всі інші поверхи є службовими. Чисельність комп'ютерів, ноутбуків, планшетів в службових приміщеннях близько 600 шт. Територія, на якій розташоване підприємство, дуже велика, в рамках території також виникає необхідність забезпечення доступу мобільних пристроїв до єдиної мережі, а також забезпечення працездатності.

Інформаційна система підприємства ТОВ "КБ "ХОРТ" є взаємопов'язаною сукупнісю засобів, методів і персоналу, які використовуються для зберігання, обробки, і видачі інформації в інтересах досягнення поставленої мети. У кожного фахівця в компанії є своє робоче місце, яке обладнане комп'ютером.

Комп'ютери підприємства не включені в єдину локальну мережу. Мережа організована тільки в рамках другого і третього поверху. Всі комп'ютери володіють однаковими характеристиками. Комп'ютери в мережі мають стандартну мережеву карту з роз'ємом RJ45 і мережеву операційну систему. В кожному кабінеті розташовані концентратори SuperStack II Hub 100 Base T4 виробництва 3Com Corp. Комп'ютери третього поверху підключаються до концентратора, що знаходиться в кабінеті у техніків на другому поверсі.

Широко застосовуються архіватори Rar, WinZip, WinRar. Всіма працівниками використовується текстовий редактор MicrosoftWord. В процесі роботи, співробітники стикаються з необхідністю детального аналізу і моніторингу всіляких даних. Тому застосування знаходить табличний процесор Microsoft Excel, який дозволяє реалізувати найбільш «популярні» методи обробки результатів соціологічних досліджень. Також на підприємстві є програмний продукт 1С: «Бухгалтерія», який є типовим рішенням для автоматизації

бухгалтерського і податкового обліку, включаючи підготовку обов'язкової звітності. На підприємстві використовується система відеоспостереження для захисту конфіденційної інформації.

На основі аналіз ризиків інформаційної безпеки можна виявити такі основні проблеми: відсутність антивірусного ПО на самих АРМ, застаріле антивірусне ПЗ на сервері, відсутність системи контролю доступу службовців до чужих АРМ, відсутність системи відеоспостереження в кабінетах, відсутність політики паролів.

На підставі оцінки ризиків найбільш цінних інформаційних активів були обрані основні завдання щодо вдосконалення інформаційної безпеки.

Забезпечення цілісності, а також конфіденційності активів можливо за рахунок впровадження антивірусного захисту. Крім того, важливо опрацювати систему спостереження, щоб вірусне і шкідливе ПЗ не могло бути принесено на флешці або іншому носії інформації.

Впровадженням системи захисту на підприємстві буде займатися системний адміністратор (підбір, установка, налагодження та обслуговування технічних і програмних засобів захисту), а також начальник служби безпеки (розробка положень, наказів, розпоряджень).

Рішення завдання забезпечення інформаційної безпеки є дуже важливою для функціонування підприємства. Втрата інформації призведе до виходу всієї системи з ладу, втрати ефективності роботи, розголошенню службової інформації.

РОЗДІЛ ІІІ. РОЗРОБКА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1. Удосконалення засобів захисту інформації на підприємстві

На основі проведеного в другому розділі аналізу була запропонована наступна система заходів для забезпечення інформаційної ТОВ "КБ "ХОРТ":

І. Технічні заходи захисту інформації

1. Апаратні засоби захисту інформації:

1) Придбати джерело безперебійного живлення для сервера.

2) Встановити відеокамери.

3) Придбати сейфи та інші пристрої для зберігання документації.

2. Програмні заходи захисту інформацій:

1) Встановити систему КУБ.

2) Встановити програмний засіб SecretNet 5.1.

3) Встановити на робочі місця користувачів антивірусні пакети. Найбільш зручною буде така система: на сервері встановлюється антивірус-сервер, а на робочих місцях - клієнтські програми, роботою яких управляє сервер. Це порівняно недороге рішення, а головне, що адміністратор зможе управляти перевіркою всіх комп'ютерів з сервера.

4) Удосконалити політику паролів. пропонувати користувачеві зміну пароля раз на місяць, рекомендувати використання складного пароля.

5) Виконати розмежування доступу до документів на сервері;

6) Виділяти різну кількість трафіку різних груп користувачів інтернету, а також визначити певний набір ресурсів, до яким можна отримати доступ.

При введенні цих заходів потрібно взяти з працівників письмову угоду про дотримання правил роботи з інформацією і технікою, які можуть бути викладені в трудовому договорі або окремим документом.

Існують три стратегії забезпечення інформаційної безпеки: оборонна, наступальна, попереджувальна.

В рамках даного підприємства обрана наступальна стратегія інформаційної безпеки. Наступальна стратегія передбачає реакцію співробітників компанії на відомі загрози, які надають вплив на інформаційну безпеку компанії.

Наступальна стратегія передбачає застосування таких заходів, як встановлення додаткових програмно-апаратних засобів аутентифікації користувачів, впровадження більш досконалих технологій розвантаження і відновлення даних, підвищення доступності системи з використанням гарячого і холодного резервування.

До організаційно-адміністративних заходів захисту інформації відносяться:

– виділення спеціальних захищених приміщень для розміщення ЕОМ і засобів зв'язку та зберігання носіїв інформації;

– виділення спеціальних ЕОМ для обробки конфіденційної інформації;

– організація зберігання конфіденційної інформації на спеціальних промаркованих магнітних носіях;

– використання в роботі з конфіденційною інформацією технічних і програмних засобів, що мають сертифікат захищеності і встановлених в атестованих приміщеннях;

– організація спеціального діловодства для конфіденційної інформації, що встановлює порядок підготовки, використання, зберігання, знищення та обліку документованої інформації;

– організація регламентованого доступу користувачів до роботі на ЕОМ, засобів зв'язку і до сховищ носіїв конфіденційної інформації;

– встановлення заборони на використання відкритих каналів зв'язку для передачі конфіденційної інформації;

– розробка та впровадження спеціальних нормативно-правових та розпорядчих документів з організації захисту конфіденційної інформації, які

регламентують діяльність усіх ланок об'єкта захисту в процесі обробки, зберігання, передачі і використання інформації;

– постійний контроль за дотриманням встановлених вимог щодо захисту інформації.

На основі аналізу існуючої системи безпеки було прийнято рішення реалізувати такі адміністративні заходи безпеки:

1) Розробити та затвердити наказом по підприємству:

- положення про захист відомостей, що містять комерційну таємницю, і іншої інформації обмеженого користування;

- інструкцію з правилами роботи з відомостями, що містять комерційну таємницю;

- інструкцію з діловодства з документами обмеженого користування.

2) Видати наказ по підприємству, в якому:

- на керівників підрозділів покласти обов'язок проведення заходів, спрямованих на забезпечення схоронності комерційної таємниці;

- визначити заходи адміністративного покарання за порушення правил роботи з документами і відомостями, що містять комерційну таємницю;

- на службу безпеки покласти обов'язок по виявленню можливих порушень, в результаті яких можливий витік охоронюваних відомостей.

3) Ввести заборону на зберігання особистої інформації на комп'ютері.

4) Встановити правила копіювання документів, що виключають виготовлення копій важливих документів без санкції керівника.

5) Від працівників, які за посадою володіють відомостями комерційної таємниці, при укладенні трудового договору брати письмові зобов'язання про нерозголошення. У разі звільнення працівника, вимагати від нього передачі всіх носіїв інформації, що становлять комерційну таємницю, які перебували в його розпорядженні.

6) Виготовити виписки, що містять витяги з положення про конфіденційної інформації для використання працівниками в повсякденній діяльності;

7) Розробити журнал обліку персональної інформації;

8) Розробити правила роботи з електронною поштою.

9) При включенні комп'ютера перед введенням пароля програмним способом видавати користувачу повідомлення, що нагадує користувачеві про правила роботи з комп'ютером.

Організаційно-адміністративні заходи захисту інформації дозволять уникнути частини ненавмисних загроз, а також навмисних загроз безпеці інформації з боку працівників підприємства. Крім того, жорсткий регламент поводження з інформаційними ресурсами дисциплінує колектив, привчає їх більш уважно працювати з даними і ставитися до них як до важливого ресурсу.

В результаті перевірки інформаційної безпеки підприємства, були виявлені основні проблеми системи відеоспостереження. З огляду на вищевикладене, розроблені заходи для підвищення ефективності функціонування системи відеоспостереження організації:

1. Заміна застарілих відеокамер.

2. Встановлення камер в приміщеннях і на прилеглій території.

3. Заміна монітора відеооператора та з'єднувального кабелю

4. Установка сервера в окремому приміщенні.

5. Установка відеомонітора біля прохідної.

6. Заміна програмного забезпечення виведення відеосигналу.

Завдяки запропонованим заходам буде побудована ефективна система відеоспостереження на підприємстві.

3.2. Розробка системи інформаційної безпеки підприємства

Для вирішення завдання забезпечення інформаційної безпеки була обрана система КУБ.

КУБ - унікальне кросфункціональне рішення для автоматизації та управління доступом до інформаційних ресурсів компанії і контролю дотримання політики безпеки.

КУБ призначений для великих компаній з великою, різнорідної КІС, з географічно розгалуженою структурою, що мають велику кількість щоденних кадрових операцій і / або високу ціну будь-яких помилок, пов'язаних з невірно наданими правами доступу до інформаційних ресурсів.

КУБ дозволяє автоматизувати управління обліковими записами, реалізувати процес узгодження прав доступу, а також забезпечити безперервний моніторинг їх змін. КУБ вирішує завдання трьох груп користувачів:

1. Підрозділам. Можливість самостійно в звичній термінології запитувати, узгоджувати і отримувати доступ до необхідним інформаційних ресурсів через web-портал; в будь-який момент часу бачити поточний статус своєї заявки.

2. Службі інформаційних технологій / автоматизації. Можливість отримувати чіткі інструкції до виконання в зрозумілих виконавцю термінах; не витрачати час на уточнення вимог заявок; бути впевненим, що своїми діями інженер не порушує політику інформаційної безпеки компанії. Можлива повна автоматизація виконання заявок.

3. Службі інформаційної безпеки. можливість безперервно контролювати всі зміни прав доступу до інформаційних ресурсів компанії та інші зміни значущих налаштувань; мати всю необхідну інформацію для оперативного розслідування інцидентів, пов'язаних з недотриманням правил політики безпеки.

Можливості системи КУБ:

1. Управління:

- Електронний документообіг заявок, електронний підпис і політика їх погоджень.

- Рольова модель управління.

- Інструменти аналізу та оптимізації ролей.

- Гнучка система звітності для різних категорій користувачів.

2. Безпека:

- Контроль за змінами прав доступу.

- Управління мережевим доступом.

- Управляння цифровими сертифікатами та контроль програмно-апаратних конфігурацій.

3. Автоматизація:

- Управління правами доступу.

- Управління обліковими даними.

На підприємстві є потреба в запровадженні антивірусного захисту, тому потрібно вибрати антивірусне програмне забезпечення.

З усіма завданнями, такими як контроль програм, інтернет-сайтів і пристроїв, впорався антивірус - Касперський. За такого важливого показника як відсоток визначення загроз антивірус Касперського показує значення більш 96%.

Антивірус Касперського можна з упевненістю вважати найкращим варіантом для захисту інформації в компанії, до того ж ціна на продукт лабораторії Касперського не є найвищою.

У компанії повинна бути розроблена стратегія антивірусної захисту. Стратегія антивірусного захисту підприємства спрямована на здійснення багаторівневого захисту всіх вразливих елементів в IT структурі організації (Рис. 3.1).

Розглянемо докладніше стратегію антивірусного захисту:

1. Інфраструктурний рівень. Вибирається структура мережі, забезпечує необхідний захист від вторгнень для найкритичніших і вразливих елементів мережі. Вона включає захист мережі від атак через установку мережевого шлюзу з файерволом корпорації, фільтрація зовнішнього трафіку мережі (в тому числі вхідних повідомлень електронної кореспонденції),

завантажуються інтернет-сторінок і служб миттєвих повідомлень, які найчастіше стають джерелами зараження.

2. Рівень програмного забезпечення. Проводиться робота по виявлення вразливих додатків, регулярне своєчасне оновлення ПО з метою закриття виявлених вразливостей. встановлюється потрібне програмне забезпечення, в залежності від потреб конкретної організації.

3. Рівень обладнання. Досліджується можливість і порядок застосування зовнішніх запам'ятовуючих пристроїв (Flash-накопичувачі, оптичні носії та інше) з метою скорочення числа можливих джерел зараження вірусами.

4. Рівень прав доступу. Регламентуються права користувачів системи, зводячи до мінімуму можливість проникнення шкідливих програм. Організовується регулярне резервне копіювання всієї критичної інформації для швидкого відновлення при необхідності.

Рис. 3.1. Стратегія антивірусного захисту

Проводиться планомірний контроль стану антивірусних програм, аудит безпеки мережі і повні антивірусні перевірки. Комплексний захист мережі від вірусів підприємства виконує наступні функції:

1. Захист персональних комп'ютерів запобігає проникненню шкідливих програм з різних джерел. так забезпечується проактивний захист від невідомих в базі вірусів.

2. Захист шлюзів і сервера електронної пошти, системи обміну email і забезпечення безпечного колективного доступу до документів компанії. Антивірус на поштовому сервері контролює і перевіряє електронну пошту, лікує

або видаляє пошкоджені файли. Система захисту не пропускає заражені листи на персональні комп'ютери, де боротися з вірусами набагато складніше.

3. Захист інтернет-трафіку. Антивірус перевіряє весь трафік, що надходить з Інтернету, і видаляє віруси. Цей етап істотно підвищує загальну захищеність мережі і є вагомим доповненням до антивірусного захисту робочих місць і серверів, але не гарантує повну безпеку.

4. Захист файлового сервера. В цьому випадку антивірус перевіряє відкриваються або змінювані файли. Проводиться розподіл системою серверних ресурсів між антивірусом і іншими серверними додатками, надаючи можливість мінімального впливу на ключові серверні служби.

5. Регулярне автоматичне оновлення ПЗ дозволяє усувати уразливості в програмних продуктах, запобігаючи зараженню, а не борючись з його наслідками.

6. Забезпечення централізованого доступу до управління елементами антивірусного захисту. Цей етап є ключовим у забезпеченні безпеки корпоративної системи.

Регулярний моніторинг всіх елементів захисту дозволяє адміністратору максимально швидко виявити проблему на одній комп'ютері, виключаючи її перехід на наступні пристрої. Відмінність персональних антивірусних програм від корпоративних рішень полягає саме в можливості централізованого моніторингу і адміністрування. Навіть в невеликих мережах така можливість необхідна для забезпечення безпеки.

3.3. Економічна ефективність

Дані для розрахунку економічного ефекту представлені в таблиці 3.1.

Таблиця 3.1

Дані для розрахунку економічного ефекту

Найменування	До впровадження	Після впровадження
Собівартість (поточні експлуатаційні витрати), грн.	609178	620190
Сумарні витрати, пов'язані з впровадженням проекту, грн.	120000	153229
Наведені витрати на одиницю робіт, руб.	118481	84448
Економічний ефект від використання розроблюваної системи, грн.	302412	

Наведені витрати на одиницю робіт після впровадження проекту складуть:

З= 620190+ 0,33 * 153229 = 670755 грн.

Наведені витрати на одиницю робіт до впровадження проекту:

З = 609178 + 0,33 * 120000 = 648778 грн.

Економічний ефект від впровадження проекту (Е) складе:

Е = 648778 * 1,5 - 670 755 = 302 412 грн.

Після визначення річного економічного ефекту розрахуємо термін окупності витрат (Т) на розробку продукту за формулою:

Т = Сумарні витрати, пов'язані з впровадженням проекту (після впровадження) / Економічний ефект від використання розроблюваної системи = 153229 / 302412 = 0.5 років.

Розрахунок фактичного коефіцієнта економічної ефективності (Еф) зробимо за формулою:

Еф = Економічний ефект від використання розроблюваної системи / Сумарні витрати, пов'язані з впровадженням проекту (після впровадження) = 302412 / 153229 = 2.

Порівняємо фактичний коефіцієнт економічної ефективності з нормативним значенням коефіцієнта ефективності капітальних вкладень (Ен = 0,33) і зробимо висновок: чим вище фактичний коефіцієнт економічної ефективності, тим швидше окупаються капітальні вкладення, здійснені в реалізацію проекту.

Таким чином, розробка і впровадження продукту, що розробляється є ефективною, так як Еф в нашому випадку вийшла більше Ен (2 більше 0,33).

У ході проробленої роботи знайдені всі необхідні дані, доводять доцільність і ефективність даної розробки. Наведемо ці дані в зведеній таблиці 3.2.

Таблиця 3.2

Таблиця економічного обґрунтування розробки та впровадження проекту

Витрати на розробку і реалізацію проекту	153229
Загальні експлуатаційні витрати	620190
Економічний ефект	302412
Коефіцієнт економічної ефективності	2
Термін окупності	0.5

Виходячи з вищевикладеного можна зробити наступний висновок: модернізація інформаційної системи безпеки буде ефективна, так як фактичний коефіцієнт економічної ефективності вийшов більше нормативного коефіцієнта.

Висновок до Розділу 3.

Для ТОВ "КБ "ХОРТ" були запропоновані наступні заходи модернізації системи інформаційної безпеки:

I. Організаційні заходи захисту інформації На підприємстві оновлені і доопрацьовані документи, регламентують питання забезпечення інформаційної безпеки. Організаційно-адміністративні заходи захисту інформації дозволять уникнути частини ненавмисних загроз, а також навмисних загроз безпеки інформації з боку працівників підприємства. Крім того, жорсткий регламент поводження з інформаційними ресурсами дисциплінує колектив, привчає їх більш уважно працювати з даними і ставитися до неї як до коштовного ресурсу.

Потрібно видати наказ по підприємству, в якому: на керівників підрозділів покласти обов'язок проведення заходів, спрямованих на забезпечення схоронності комерційної таємниці; визначити заходи адміністративного покарання за порушення правил роботи з документами і відомостями, що містять комерційну таємницю; на службу безпеки покласти обов'язок по виявленню можливих порушень, в результаті яких можливий витік охоронюваних відомостей.

Також треба ввести заборону на зберігання особистої інформації на комп'ютері та встановити правила копіювання документів, що виключають виготовлення копій важливих документів без санкції керівника.

II. Технічні заходи захисту інформації.

Модернізована система відеоспостереження забезпечує надійний захист об'єкта від несанкціонованого проникнення і повністю відповідає вимогам підприємства в сфері відеоспостереження.

При виборі технічних засобів особлива увага приділялася їх функціональних характеристик і технічної взаємодії між різними пристроями один з одним. Крім того, закуплено і встановлено сейфи для зберігання конфіденційною і внутрішньої інформації.

III. Програмні заходи захисту інформації:

На підприємстві є потреба організації комплексного антивірусного захисту. На основі аналізу було обрано програмне засіб «Kaspersky Endpoint

Security для бізнесу розширений». Найбільш зручною буде така система антивірусного захисту: на сервері встановлюється антивірус-сервер, а на робочих місцях – клієнтські додатки, роботою яких керує сервер. це порівняно недороге рішення, а головне, що адміністратор зможе управляти перевіркою всіх комп'ютерів з сервера.

Крім того, спланована установка системи КУБ, яка забезпечить комплексне рішення проблем забезпечення безпеки інформації.

Модернізація інформаційної системи безпеки буде ефективна, так як фактичний коефіцієнт економічної ефективності вийшов більше нормативного коефіцієнта.

ВИСНОВКИ

Інформаційна безпека - практика запобігання несанкціонованому доступу, використання, розкриття, спотворення, зміни, дослідження, записи або знищення інформації.

Це універсальне поняття застосовується незалежно від форми, яку можуть приймати дані (електронна або, наприклад, фізична). Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації.

В основі інформаційної безпеки лежить діяльність по захисту інформації - забезпечення її конфіденційності, доступності та цілісності, а також недопущення будь-якої компрометації в критичній ситуації.

Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту (СЗІБ). Для побудови та ефективної експлуатації СЗІБ необхідно: виявити вимоги захисту інформації, специфічні для даного об'єкта захисту; врахувати вимоги національного та міжнародного законодавства; використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ; визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ; розподілити між підрозділами області відповідальності в здійсненні вимог СЗІБ; на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові Політику інформаційної безпеки об'єкта захисту; реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-апаратні, інженерно-технічні та інші способи і засоби захисту інформації; реалізувати систему менеджменту (управління) інформаційної безпеки.

ISO / IEC 27001 - міжнародний стандарт по інформаційної безпеки, розроблений спільно Міжнародною організацією зі стандартизації та Міжнародної електротехнічної комісією.

Підготовлений до випуску підкомітетом SC27 Об'єднаного технічного комітету JTC 1. Стандарт містить вимоги в області інформаційної безпеки для створення, розвитку та підтримки Системи менеджменту інформаційної безпеки (СМІБ).

ISO 27001 може бути впроваджений в будь-якій організації: комерційної або некомерційної, приватної або державної, маленької чи великої. Він був написаний провідними світовими експертами в області інформаційної безпеки і пропонує методологію для впровадження управління інформаційною безпекою на підприємстві.

Він також дозволяє компаніям отримати сертифікацію, що означає, що незалежний орган із сертифікації підтвердить, що організація впровадила інформаційну безпеку відповідно до стандарту ISO 27001.

У стандарті ISO / IEC 27001 (ISO 27001) зібрані описи найкращих світових практик в області управління інформаційною безпекою. ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення Системи Менеджменту Інформаційної Безпеки (СМІБ).

Основними принципами стандарту ISO 27001 є: конфіденційність інформації, цілісність інформації, доступність інформації.

В рамках стандартів міжнародного (стандарти ISO) та національного рівнів (ДСТУ, НД ТЗІ) щодо інформаційної безпеки визначаються вимоги до захисту інформації, або її властивостей.

Міжнародна стандартизація складових системи управління інформаційною безпекою формує три напрямки розвитку в сфер СМІБ: сімейство стандартів „Методи забезпечення безпеки” – ISO/IEC 27000-ISO/IEC 27037; сімейство стандартів „Методи та засоби забезпечення безпеки” – ISO/IEC 15408 („За-

гальні критерії", 3 частини), ISO/IEC 13335 (5 частин), ISO/IEC 18045; сімейство стандартів „Управління та аудиту інформаційних технологій" (CobIT, ITSM, ITIL та ін.)

Питання ефективної реалізації будьякого стандарту невід'ємне від його інструментальних можливостей, що дозволяє автоматизувати роботу, забезпечити гнучкість і адаптивність застосування різноманітних "паперових" методик.

Найкращими можливостями в цьому плані володіє стандарт ISO/IEC 27002: 2005 (ISO 17799). Виходячи з зазначеного, доцільно доповнити діючі та перспективні стандарти такими програмними продуктами як довідник з питань інформаційної безпеки, гіпертекстовий довідник з питань захисту інформації, керівництво для співробітників служби безпеки, різноманітні демонстраційні версії і презентації, зручною навігацією.

В ході оцінки ризику можна оцінити, як частоту виникнення небажаних подій і ймовірність того, що якийсь дана подія може завдати шкоди ресурсу, так і найголовніше - вартість даного збитку.

При оцінці ризиків ІБ можна виділити недоліки: оцінка носить практично завжди формальний характер; оцінюється без розслідування на випадкової, а не постійній основі. Це впливає на те, що існуючі важливі дані залишаються неврахованими і обізнаність осіб, які приймають, якесь рішення по ліквідації ризиків у багатьох організаціях буде недостатньою. Необхідно так само пам'ятати, що головний ризик - це людина, яка надає для ІБ найбільшу небезпеку в навмисній або не навмисній помилці.

Так як відсутні загальноприйняті підходи і методики для оцінки ризиків і в кожному конкретному випадку необхідно ретельно прораховувати і продумувати всі фактори ризику, проводити аналіз і розрахунок, що є дуже трудомістким завданням, крім того ще й існує ймовірність отримати помилковий результат.

З усіх методів оцінки ризиків необхідно застосовувати сукупність методів аналізу, обробки інформації та тільки після цього оцінювати ризики ІБ, і

здійснювати управління ІБ. Так само необхідно зменшувати «ручну працю», використовувати існуючі сучасні методології оцінки ризиків, і все більше переходити до оцінки ризиків за допомогою інтелектуального аналізу даних нейронних мереж.

Об'єктом дослідження в дипломній роботі є ТОВ "КБ "ХОРТ". Основна форма діяльності – діяльність у сфері оборони.

Підприємство займає споруду площею близько 50 000 квадратних метрів і висотою в 7 поверхів. На першому поверсі будівлі знаходиться кафетерій з інтернет доступом. Всі інші поверхи є службовими. Чисельність комп'ютерів, ноутбуків, планшетів в службових приміщеннях близько 600 шт. Територія, на якій розташоване підприємство, дуже велика, в рамках території також виникає необхідність забезпечення доступу мобільних пристроїв до єдиної мережі, а також забезпечення працездатності.

Інформаційна система підприємства ТОВ "КБ "ХОРТ" є взаємопов'язаною сукупнісю засобів, методів і персоналу, які використовуються для зберігання, обробки, і видачі інформації в інтересах досягнення поставленої мети. У кожного фахівця в компанії є своє робоче місце, яке обладнане комп’ютером.

Комп'ютери підприємства не включені в єдину локальну мережу. Мережа організована тільки в рамках другого і третього поверху. Всі комп'ютери володіють однаковими характеристиками. Комп'ютери в мережі мають стандартну мережеву карту з роз'ємом RJ45 і мережеву операційну систему. В кожному кабінеті розташовані концентратори SuperStack II Hub 100 Base T4 виробництва 3Com Corp. Комп'ютери третього поверху підключаються до концентратора, що знаходиться в кабінеті у техніків на другому поверсі.

Широко застосовуються архіватори Rar, WinZip, WinRar. Всіма працівниками використовується текстовий редактор MicrosoftWord. В процесі роботи, співробітники стикаються з необхідністю детального аналізу і моніторингу всіляких даних. Тому застосування знаходить табличний процесор

Microsoft Excel, який дозволяє реалізувати найбільш «популярні» методи обробки результатів соціологічних досліджень. Також на підприємстві є програмний продукт 1С: «Бухгалтерія», який є типовим рішенням для автоматизації бухгалтерського і податкового обліку, включаючи підготовку обов'язкової звітності. На підприємстві використовується система відеоспостереження для захисту конфіденційної інформації.

На основі аналіз ризиків інформаційної безпеки можна виявити такі основні проблеми: відсутність антивірусного ПО на самих АРМ, застаріле антивірусне ПЗ на сервері, відсутність системи контролю доступу службовців до чужих АРМ, відсутність системи відеоспостереження в кабінетах, відсутність політики паролів.

Для ТОВ "КБ "ХОРТ" були запропоновані наступні заходи модернізації системи інформаційної безпеки:

I. Організаційні заходи захисту інформації На підприємстві оновлені і доопрацьовані документи, регламентують питання забезпечення інформаційної безпеки. Організаційно-адміністративні заходи захисту інформації дозволять уникнути частини ненавмисних загроз, а також навмисних загроз безпеки інформації з боку працівників підприємства. На основі аналізу існуючої системи безпеки було прийнято рішення реалізувати такі адміністративні заходи безпеки:

Розробити та затвердити наказом по підприємству: положення про захист відомостей, що містять комерційну таємницю, і іншої інформації обмеженого користування; Інструкцію з правилами роботи з відомостями, що містять комерційну таємницю; інструкцію з діловодства з документами обмеженого користування.

Видати наказ по підприємству, в якому: на керівників підрозділів покласти обов'язок проведення заходів, спрямованих на забезпечення схоронності комерційної таємниці; визначити заходи адміністративного покарання за порушення правил роботи з документами і відомостями, що містять комерційну

таємницю; на службу безпеки покласти обов'язок по виявленню можливих порушень, в результаті яких можливий витік охоронюваних відомостей.

Ввести заборону на зберігання особистої інформації на комп'ютері. Встановити правила копіювання документів, що виключають виготовлення копій важливих документів без санкції керівника. Від працівників, які за посадою володіють відомостями комерційної таємниці, при укладенні трудового договору брати письмові зобов'язання про нерозголошення. У разі звільнення працівника, вимагати від нього передачі всіх носіїв інформації, що становлять комерційну таємницю, які перебували в його розпорядженні.

Виготовити виписки, що містять витяги з положення про конфіденційної інформації для використання працівниками в повсякденній діяльності; Розробити журнал обліку персональної інформації; Розробити правила роботи з електронною поштою. При включенні комп'ютера перед введенням пароля програмним способом видавати користувачу повідомлення, що нагадує користувачеві про правила роботи з комп'ютером.

II. Технічні заходи захисту інформації.

Модернізована система відеоспостереження забезпечує надійний захист об'єкта від несанкціонованого проникнення і повністю відповідає вимогам підприємства в сфері відеоспостереження.

При виборі технічних засобів особлива увага приділялася їх функціональних характеристик і технічної взаємодії між різними пристроями один з одним. Крім того, закуплено і встановлено сейфи для зберігання конфіденційною і внутрішньої інформації.

III. Програмні заходи захисту інформації:

На підприємстві є потреба організації комплексного антивірусного захисту. На основі аналізу було обрано програмне засіб «Kaspersky Endpoint Security для бізнесу розширений». Найбільш зручною буде така система антивірусного захисту: на сервері встановлюється антивірус-сервер, а на робочих

місцях – клієнтські додатки, роботою яких керує сервер. це порівняно недороге рішення, а головне, що адміністратор зможе управляти перевіркою всіх комп'ютерів з сервера.

Крім того, спланована установка системи КУБ, яка забезпечить комплексне рішення проблем забезпечення безпеки інформації.

Модернізація інформаційної системи безпеки буде ефективна, так як фактичний коефіцієнт економічної ефективності вийшов більше нормативного коефіцієнта.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основи інформаційного права України: навч. посіб. / Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін.; За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К.: Знання, 2004. 274 с.

2. Пахнін М.Л. Особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. 2014. Вип. 4. С. 414- 422.

3. Цимбалюк В. Сутність інформаційної безпеки в умовах входження України до глобальної кіберцивілізації. Науковий вісник Нац. академії Держ. податк. служби України. 2004. № 4(26). С. 135–141.

4. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. Віче. 2007. №12. С. 23-25.

5. Конституція України. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

6. Закон України «Про державну таємницю». Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

8. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12&p=1217856518710949#Text

9. Шаріпова Н.А. Інформаційне забезпечення напрямків маркетингової діяльності підприємства // Сибірський торгово-економічний журнал. 2012. № 16. С. 83-87.

10. Інформаційна безпека людини:теорія і практика : монографія. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

11. Цимбалюк В. С. Безпека як інститут інформаційного права та його місце в структурі кодифікації інформаційного законодавства Моделювання

колективної безпеки: інформаційний вимір: Мат. міжн. «круглого столу» (м. Київ, 27 квітня 2011 р.). К.: Вид-во «Академпрес», 2011. С. 28–32.

12. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

13. Левченко О.В. Проблеми і шляхи формування системи інформаційної безпеки держави. Зб. наук. праць Харків. ун-ту Повітряних Сил. 2014. Вип. 2(39). С. 166.

14. Шаріпова Н.А. Інформаційне забезпечення територіального бренду - У збірнику: Сталий розвиток регіону: минуле, сучасне, майбутнє. Міжнародна науково-практична конференція студентів, аспірантів, викладачів, теоретиків і практиків. Омськ, 2012. С. 127-130.

15. Information Security Management System. URL: https://otrs.com/otrs-solutions/isms/

16. Інформаційна безпека людини:теорія і практика : монографія. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

17. General Data Protection Regulation. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

18. Залізняк В.А. Інформаційна безпека. Актуальні проблеми зміцнення державності і національної єдності України: матеріали наук.-практ. конференції. Київ, 2010. С. 46.

19. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім “Києво-Могилянська академія”, 2015. – 497 с.

20. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис.на здобуття наук ступеня канд. екон. наук: 08.00.04//М.Ю. Танцюра.- Сімферополь, 2012.- С. 21.

21. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки. – 2010. – № 2. – Т. 2. – С. 32.

22. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) //Підприємництво, господарство і право. – 2014. - №3. - С.88.

23. Лук'яненко Д. Г. Стратегії глобального управління. Міжнародна економічна політика. – 2009. – № 8-9. – С. 43.

24.Качан О.І. Інформаційна безпека підприємств. Національний університет водногогосподарства та природокористування, м. Рівне. 2019. С. 4.

25. A History Of Information Security. URL: https://www.ifsecglobal.com/cyber-security/a-history-of-information- security/

26. Марунич А. В. Захист інформації як основна складова економічної безпеки підприємства / А. В. Марунич // Управління розвитком. — 2014. — № 14. — С. 130.

27. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України: монографія. Харків: АМ-Фенікс, 2018. 289 с.

28. Система менеджменту інформаційної безпеки ISO / IEC 27001: 2005. URL: http://www.tuev-nord.com.ua/index.php/sertsm / isoiec-27001

29. Бурячок В. Л., Толюпа С. В., Семко В. В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ: ДУТ-КНУ, 2016. 178 с.

30. ISO/IEC 27001:2013. URL: http:// intercert.com.ua/articles/posts/292-standartiso-iec-27001-2013

31. Управління інформаційною безпекою ISO / IEC 27001: 2013 URL: http://tmsua.com/standarts/iso-27001-2013/

32. ISO / IEC 27002. URL: https://pqm-online.com/assets/files/pubs.pdf

33. ISO / IEC 27004. URL: https://www.iso.org/standard/64120.html

34. ISO / IEC 27005. URL: https://www.iso27001security.com

35. ISO 22301. URL: https://www.iso.org/files/live/ PUB100442.pdf

36. ISO 9001. URL: https://www.iso.org/standard/62085.html

37. Овсяніков В.В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки. Modern Information Technologies in the Sphere of Security and Defence № 3(24)/2015. С. 192.

38. ISO/IEC 27000-ISO/IEC 27037. URL: https://www.iso27001s.html

39. ISO/IEC 15408. URL: https://www.iso.org/standard/50341.html

40. ISO/IEC 18045. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-18045

41. ДСТУ СУІБ 1.0/ISO/IEC 27001:2010 „Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги". URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

42. ДСТУ СУІБ 2.0/ISO/IEC 27002: 2010 „Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

43. ISO/IEC 27005. URL: https://www.iso.org/obp/:iso-iec:27005:en

44. ISO/IEC 27003:2010. URL: https://www.iso.org/standard/42105.html

45. Герасименко В.А., Малюк А.А. Основи захисту інформації. М .: Інкомбук, 1997. С. 65.

46. Логінова Н. І., Джобожур Р. Р. Правовий захист інформації: навчальний посібник. Одеса: Фенікс, 2015. 264 с.

47. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління: навчальний посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

48. Маслова М.А. Аналіз і визначення ризиків інформаційної безпеки // Науковий результат. Інформаційні технології. Т. 4. № 1, 2019. С. 26.

49. Тенетко М.І., Пєскова О.Ю. Аналіз ризиків інформаційної безпеки // Відомості ПФУ. Технічні науки, 2011. № 12. С. 45.

50. Fisher T. Free and Public DNS Servers. Lifewire. URL: https://www.lifewire.com/free-and-public-dnsservers-2626062

51. Global Cybersecurity Index (GCI) 2018. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

52. NIST Special Publication 800-63B URL: https://pages.nist.gov/800-63-3/sp800-63b.html

53. International Standard ISO/IEC 27000, 2009 y. URL: http://pqmonline.com/assets/files/lib/std/iso_iec_27000-2009.pdf

54. СЕРТИФІКАЦІЯ ISO/IEC 27001. URL: https://iitc.com.ua/ru/sertifikatsiya/sertifikatsiya-iso-27001/

55. ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

56. Стандарт ISO/IEC 27001. URL: https://intercert.com.ua/articles/posts/292-standart-iso-iec-27001

57. Офіційна сторінка товариства з обмеженою відповідальністю КБ ХОРТ. URL: https://youcontrol.com.ua/catalog/company_details/40336546/

58. Домарєв В.В., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навч. пос. К.: НАУ, 2006. 108 с.

ДОДАТКИ

Додаток А.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій
та управління якістю продукції АПК

XII МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ ВЧЕНИХ, АСПІРАНТІВ І СТУДЕНТІВ

«Наукові здобутки у вирішенні актуальних
проблем виробництва та переробки сировини,
стандартизації і безпеки продовольства»

присвячена 15-ти річчю факультету харчових технологій
та управління якістю продукції АПК

ЗБІРНИК ПРАЦЬ

за підсумками
XII Міжнародної науково-практичної
конференції вчених, аспірантів і студентів

КИЇВ – 2024

3.Про захист прав споживачів: Закон України: від 12.05.1991 зі змінами та доповненнями від 19.11.2022 №1023-XII. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1023-12#Text

4.Про основні принципи та вимоги до безпечності та якості харчових продуктів : Закон України від 23.12.1997 № 771/97-ВР зі змінами та доповненнями від 26.10.2023 №3221-IX. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/771/97-%D0%B2%D1%80

5.Русавська В. А. Системи НАССР в закладах ресторанного бізнесу України: нормативно-правове регулювання. *Гостинність, сервіс, туризм: досвід, проблеми, інновації* : тези доп. X Міжнар. наук.-практ. інтернет-конф., Київ, 6-7 квіт., 2023 р. Київ, 2023. 535 с. С. 65-68. URL: https://fgritb.knukim.edu.ua/home/konferencii.html

УДК 004.056

І.В. Злобін, студент магістратури
Т.В. Науменко, доктор філософії (PhD), доцент
А.В. Антоненко, к.т.н., доцент
Національний університет біоресурсів і природокористування України, м. Київ

РОЗРОБЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ОРГАНІЗАЦІЇ

Розроблення системи управління інформаційною безпекою (ІБ) в організації - це ключовий етап для забезпечення захисту конфіденційності, цілісності та доступності даних та інформаційних ресурсів. Ось деякі кроки, які можна виконати при розробленні такої системи:

Аналіз загроз і ризиків: Провести оцінку загроз і ризиків інформаційної безпеки, враховуючи потенційні загрози зовнішніх зловмисників, внутрішній недбалості або недоліків у системі.

Визначення політик безпеки: Створити політики і процедури щодо захисту даних, доступу до інформаційних ресурсів, обмежень щодо використання засобів інформаційної технології.

Захист інфраструктури: Забезпечити захист інформаційної інфраструктури за допомогою файрволів, антивірусного програмного забезпечення, систем виявлення вторгнень тощо.

Навчання персоналу: Провести навчання та пояснення персоналу щодо важливості безпеки і правил обробки інформації.

Відповідність законодавству: Враховувати вимоги законодавства, які стосуються захисту даних, зокрема GDPR, HIPAA та ін.

Аудит і моніторинг: Здійснювати періодичний аудит і моніторинг системи ІБ для виявлення можливих вразливостей та виявлення несанкціонованих дій.

Реагування на інциденти: Розробити процедури реагування на інциденти безпеки, включаючи плани відновлення після кризи та відновлення даних.

Постійне вдосконалення: Систему управління ІБ слід постійно вдосконалювати відповідно до змін у загрозах, технологіях та внутрішніх процесах організації.

Розроблення і реалізація цих заходів допоможе забезпечити ефективний рівень захисту інформації в організації та запобігти можливим інцидентам безпеки.

ЛІТЕРАТУРА

Як стандарт ISO/IEC 27001 допомагає розвиватися сучасному бізнесу URL: https://my-itspecialist.com/standard-iso/iec-27001-for-business

УДК 637.1:006.44

А.О. Ігрін, студент магістратури
Т.В. Науменко, доктор філософії (PhD), доцент
Т.В. Бровенко, к.т.н., доцент
Національний університет біоресурсів і природокористування України, м. Київ

РОЗРОБЛЕННЯ ЕЛЕМЕНТІВ НАССР В УМОВАХ МОЛОКОПЕРЕРОБНОГО ПІДПРИЄМСТВА

Система НАССР (Hazard Analysis and Critical Control Points) - це система аналізу ризиків та критичних точок контролю, яка використовується для забезпечення безпечності харчових продуктів. Нижче наведено кілька елементів НАССР, які можна розробити для молокопереробного підприємства:

Аналіз потенційних ризиків: Проведення оцінки ризиків для ідентифікації потенційних небезпек та ризиків, що пов'язані з процесами молокоперероблення, такими як небезпечні хімічні речовини, термічні процеси, механічні ускладнення та інші.

Встановлення стандартів безпеки: Розроблення стандартів та процедур щодо безпеки праці, які повинні бути дотримані під час виробничих процесів на молокопереробному підприємстві.

Навчання персоналу: Проведення навчання та підготовки працівників щодо правильних методів та процедур безпеки праці, включаючи роботу з обладнанням, робочими матеріалами та хімікатами.

Міністерство освіти і науки України
Національний університет біоресурсів і природокористування України

СЕРТИФІКАТ

ПІДТВЕРДЖУЄ, ЩО

Злобін І.В.

взяв(ла) участь у

XII Міжнародній Науково-практичній конференції вчених, аспірантів і студентів «НАУКОВІ ЗДОБУТКИ У ВИРІШЕННІ АКТУАЛЬНИХ ПРОБЛЕМ ВИРОБНИЦТВА ТА ПЕРЕРОБКИ СИРОВИНИ, СТАНДАРТИЗАЦІЇ І БЕЗПЕКИ ПРОДОВОЛЬСТВА»

присвяченої 15-ти річчю факультету харчових технологій та управління якістю продукції АПК

Проректор з науково-педагогічної роботи Оксана ТОНХА

м. Київ, 18-19 квітня 2024 року