МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ І ПРИКЛАДНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ

ГОЙ ВІКТОРІЯ ОЛЕГІВНА

Допускається до захисту:
в. о. завідувача кафедри
інформаційних систем управління,
д. е. н., професор
_____ Ольга АНІСІМОВА
« _____ « _____ 20__р.

МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЇ ТА ДОКУМЕНТАЦІЇ НА ПІДПРИЄМСТВІ

Спеціальність 029 «Інформаційна, бібліотечна та архівна справа»

Кваліфікаційна (магістерська) робота

Науковий керівник:
Анісімова О.М., в.о. завідувача кафедри
інформаційних систем управління,
д-р екон. наук, професор

Оцінка: _____ / _____ / _____
(бали / за шкалою EKTS / за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця – 2024

Гой В. О. Механізм захисту інформації та документації на підприємстві. Спеціальність 029 «Інформаційна, бібліотечна та архівна справа». Донецький національний університет імені Василя Стуса, Вінниця, 2024. 79 с.

У магістерській роботі досліджено теоретико-методичні засади захисту інформації та документації на підприємстві, які є види й джерела загроз для інформації та документації. Розглянуто важливість питання створення захисту інформації на підприємстві. Проаналізовано, які методи захисту інформації використовує компанія «Макош», досліджено проблемні аспекти компанії, а також розроблено механізм захисту документів, як паперових так і електронних. Особлива увага приділена методам ефективного налагодження систем захисту в організаціях й компаніях.

Ключові слова: захист інформації, документація, інформація, організація захисту, механізм захисту інформації.

Табл. 1. Рис. 17. Дод. 1. Бібліограф: 46 найм.

Hoi Viktoria. **Mechanism of information and documentation protection at the enterprise.** Specialty 029 «Information, library and archive studies», Vasyl' Stus Donetsk National University, Vinnytsia, 2024. 79 p.

The master's thesis researched the theoretical and methodological principles of information and documentation protection at enterprises, which are a source of threats to information and documentation. Considered the importance of creating information protection at enterprises. The methods of information protection used by the company «Makosh» were analyzed, problematic aspects of the company were investigated, and a mechanism for protecting documents, both paper and electronic, was developed. Special attention is paid to the methods of effective adjustment of the protection system in organizations and companies.

Keywords: information protection, documentation, information, protection organization, information protection mechanism.

Table 1. Fig. 17. Add. 1. Bibliography: 46 items.

ЗМІСТ

ВСТУП

Актуальність теми. Безперечно, ключове місце в діяльності індивідів і суспільства в цілому сьогодні посідає – інформація і все, що з нею пов'язано: створення, обмін, використання, знищення. Мабуть, це один із найцінніших ресурсів для виживання людини

Володіння певною інформацією може призвести до нерозкритих можливостей людини, а втрата певної інформації може призвести до незворотних наслідків. Тому одним із найсерйозніших питань, пов'язаних з інформаційними операціями, є забезпечення безпеки цих операцій.

Інформація може бути викрадена або змінено неналежним чином або навіть втрачено під сильним впливом. Задля мінімізації ризиків постійно створюються та вдосконалюються методи запобігання та протидії негативним факторам, що впливають на інформацію. Тому з’явилися різноманітні нормативні документи та стандарти, однією з цілей яких є підвищення рівня інформаційної безпеки.

Захист документації, інформаційних ресурсів є одним із важливий та пріоритетних завдань безпеки підприємств у світі й звичайно України, оскільки перехід до інформаційного суспільства змінив поняття (статус) інформації. На даний момент вона може бути як засобом забезпечення безпеки, так і загрозою і небезпекою.

Загальнотеоретичним питанням формування механізму захисту інформації і використання методик з метою захисту інформації на підприємствах присвячено роботи багатьох авторів, а саме: В. В. Микитенко, В. В. Бут, О. В. Гребенюк, М. О. Живко, В. С. Цимбалюк, О. А. Сороківська, А. М. Чорна. Безпека інформаційних систем є одним із питань, яке привертає велику увагу з боку аналітиків, інженерів та інших фахівців в сфері інформаційно безпеки. Проте невирішеним питанням у сфері захисту інформації залишається, адже у сучасному світі використовують вже сучасні механізм, або ж взагалі не використовують, тому що не придають цьому великого значення.

Мета дослідження полягає в тому, щоб, спираючись на аналіз основних складових захисту інформації на підприємстві та методів формування ефективної системи механізму у компанії «Макош», виявити проблематику, донести важливість захисту документації та запропонувати, розробити ефективний механізм захисту інформації у компанії.

Досягнення поставленої мети вимагало вирішення наступних *завдань*:

- дослідити загальну, базову термінологію захисту інформації на підприємствах;
- розглянути особливості організації системи захисту інформації на підприємствах;
- виділити джерела загроз системи захисту інформації;
- провести аналіз ефективності системи захисту інформації на підприємствах;
- охарактеризувати, описати загальні дані та інформацію про обране підприємство;
- виокремити проблематику організацію захисту інформації у компанії «Макош»;
- виявити взаємозв'язок організації системи захисту інформації з ефективною діяльністю підприємства;
- виявити методи удосконалення системи захисту інформації у компанії «Макош»;
- розробити механізм захисту інформації та документації у компанії «Макош»

Об'єкт дослідження – захист інформації та документації на підприємстві.

Предмет дослідження – механізм захисту інформації та документації у компанії «Макош».

Методи дослідження для формування базової інформації про захист інформації на підприємстві було використано опрацювання літератури за даною темою, аналіз, порівняння й спостереження.

Теоретичне та практичне значення одержаних результатів. Результати дослідження можуть використовуватись в діяльності підприємств різних форм власності для підвищення ефективності існуючої системи захисту інформації, зокрема на підприємстві, що досліджувалось.

Апробація результатів дослідження. Результати проведеного наукового дослідження було обговорено у рамках таких конференцій:

Гой В. О., Анісімова О. М. «Особливості захисту інформації на підприємстві»». *Прикладні аспекти сучасних міждисциплінарних досліджень*: Збірник матеріалів II Всеукраїнської науково-практичної конференції *(24 листопада 2023 р., м. Вінниця).* Вінниця: ДонНУ імені Василя Стуса, 2023. С. 18-20.

Положення, що виносяться на захист. В магістерській роботі автором досліджено теоретичні засади захисту інформації; визначено проблеми у системі захисту інформації на підприємстві; побудовано механізм захисту інформації; внесено пропозиції щодо вдосконалення організації захисту інформації у компанії «Макош».

Структура роботи. Магістерська кваліфікаційна робота складається зі вступу, трьох основних розділів, висновків, списку використаних посилань з 46 найменувань. Загальний обсяг становить 79 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ

1.1. Основні поняття та сутність захисту інформації

У нових реаліях сьогодення в усьому світі, у кожній країні важливу роль має захист інформації, починаючи від державними установами, закінчуючи усіма маленькими структурами, організаціями та підприємствами. Оскільки, збільшились кількості кіберзагроз, обсяги важливості даних, розширення віртуальних робочих середовищ (наприклад, дистанційна робота, віддалена), регулярні вимоги (багато країн впроваджують строгі вимоги, саме щодо захисту та конфіденційності інформації), залежність від IT-інфраструктури, підвищена увагу громадськості до закритої інформації, саме ці фактори вимагають звернути увагу на захист інформації.

Інформація – це набір даних, який має значення або сенс для людини. Це не просто факти чи цифри, а сформована і оброблена інтерпретація даних, яка може передавати зміст, повідомлення або розуміння. [1]

Інформація – це загальне абстрактне поняття, яке має різні значення залежно від ситуації. Походить від латинського слова «informatio», яке має такі варіанти значень:

- роз'яснення;
- виклад фактів та подій;
- тлумачення;
- представлення та поняття;
- ознайомлення. [46]

Іншими словами, це те, що має потенційності впливати на знання, рішення або стан особи чи організації. Інформація може бути подана у різних формах,

таких як текст, зображення, звук, та інші, і грає важливу роль у процесі комунікації та прийняття рішень.

Найважливішими, з практичної точки зору, властивостями інформації є Цінність інформації – визначається забезпеченням можливості досягнення мети, поставленої перед отримувачем інформації.

Достовірність – це отримана інформація яка відповідає об'єктивній реальності навколишнього світу.

Актуальність – це вимір відповідності важливості та достовірності інформації поточному часу (певному часовому періоду). [2]

Для людини інформація поділяється на види залежно від типу рецепторів, що сприймають її.

На рисунку 1 наведено види інформації:

Рисунок 1.1 – Види інформації

Візуальна інформація – сприймається органами зору.

Аудіальна інформація – сприймається органами слуху. Тактильна – сприймається тактильними рецепторами.

Нюхова інформація – сприймається нюховими рецепторами.

Смакова інформація – сприймається смаковими рецепторами.

За формою подання інформація ділиться на такі види:

Текстова – та, яка передається у вигляді символів, призначених позначати мову;

Числова – та, яка передається у вигляді цифр і знаків, що використовують у математичних діях;

Графічна – та, яка передається у вигляді зображень, подій, предметів, графіків;

Звукова – та, що передається усно або у вигляді запису передачі лексем мови аудіальним шляхом.

За призначенням інформацію також ділять на такі види:

Масова – тривіальні відомості, що оперують набором понять, зрозумілі більшій частині соціуму.

Спеціальна – специфічні поняття, при використанні відбувається передача даних, які можуть бути не завжди зрозумілі основній масі соціуму, але потрібні і зрозумілі в рамках вузьких соціальних груп, де використовується дана інформація.

Особиста – набір відомостей про певну особистість, яка визначає соціальний стан і типи соціальних взаємодій всередині популяції [3].

У законодавстві Україна виділяють інформацію з обмеженим доступом. Інформацією з обмеженим доступом є:

- конфіденційна,
- таємна
- службова інформація.

Інформація з обмеженим доступом – інформація, яка має право доступу до якої обмежене встановленими правовими нормами, правилами.

Таємна інформація (secret information) – інформація з обмеженим доступом, яка містить дані, які становлять державну чи іншу передбачену законодавством таємницю і розповсюдження якої завдає шкоди особі, суспільству та державі [4].

Конфіденційна інформація – інформація з обмеженим доступом, що містить відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб або держави, і порядок доступу до якої встановлюється ними.

Конфіденційність інформації – інформація доступ до якої є обмежений, інформація не може бути отримана неавторизованим користувачем і процесом в тій чи іншій сфері [5].

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Тому, важливо розуміти, що таке захист інформації, правила, проблеми, джерела та її основні поняття й сутність захисту.

Захист інформації – це система заходів і політик, призначених для забезпечення конфіденційності, цілісності та доступності інформації та запобігання несанкціонованому доступу, знищенню чи неправомірному використанню [6].

Захист інформації - це комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та забезпечення безпеки інформації. Залежно від виду загрози інформаційну безпеку можна розглядати як стан захищеності людини, суспільства і країни від неякісної інформації; інформації та інформаційних ресурсів від неправомірного впливу третіх осіб; інформаційні права і свободи людини і громадянина. [41] .

Захист – засіб для обмеження доступу чи використання всієї або частини обчислювальної системи; юридичні, організаційні та технічні, в тому числі програмні, заходи запобігання несанкціонованого доступу до апаратури, програм і даних.

У наукових джерелах розглядається ряд методів, задля захисту інформаційної системи. Зокрема виділяють:

- законодавчі (нормативні акти, закони , стандарти);

- адміністративні (дії організації, що робляться керівництвом);

- процедурні (конкретні заходи безпеки, що мають діяльність з певними людьми);

- програмно-технічні (для ідентифікації і перевірки користувачів; управління доступом; протоколювання і аудиту; криптографії; екранування та інші).

Апаратно-програмні засоби захисту - засоби, в яких програмна і апаратна частини повністю взаємопов'язані і нероздільні. Апаратні засоби захисту - це електронні, електромеханічні та інші пристрої, які вбудовані безпосередньо в блоки автоматизованої інформаційної системи або виконані як самостійні пристрої, які здійснюють зв'язок з цими блоками. Вони використовуються для внутрішнього захисту комп’ютерного обладнання та структурних елементів системи, наприклад: терміналів, процесорів, периферійних пристроїв, ліній зв’язку тощо.[7]

Інформаційна безпека (ІБ) – стан захищеності життєво важливих інтересів людини, суспільства і країни, запобігання завданню шкоди внаслідок використання неповної, несвоєчасної та недостовірної інформації, негативного інформаційного впливу, негативних наслідків використання інформаційних технологій, невиконання Авторизованого розповсюдження. , використання та порушення цілісності, конфіденційності та доступності інформації [8]

Виходячи з даного визначення можемо сказати, що ІБ підприємства включає в себе систему заходів, спрямованих на захист інформаційного простору і персональних даних від випадкового або навмисного їх пошкодження, крадіжки або внесення змін, а також захист бізнес процесів.

Основні поняття та сутність захисту інформації наведено на рис. 1.2.

1. Конфіденційність:

•Обмеження доступу: Заходи, спрямовані на заборону доступу до інформації неуповноваженим особам.

•Шифрування: Застосування криптографічних методів для захисту інформації від несанкціонованого доступу.

2. Цілісність:

•Захист від змін: Забезпечення того, щоб інформація не піддавалася недозволеним змінам або маніпуляціям.

•Цифровий підпис: Використання цифрових підписів для перевірки цілісності інформації.

Рисунок 1.2 – Основні поняття та сутність захисту інформації

3. Доступність:

•Забезпечення доступу: Заходи для гарантування того, що інформація буде доступною тим, хто має на це право.

•Резервне копіювання: Зберігання резервних копій даних для відновлення доступу у випадку аварій чи втрати інформації.

4. Аутентифікація:

•Перевірка особи: Визначення і підтвердження ідентичності користувача або системи.

•Багаторівнева аутентифікація: Використання декількох методів аутентифікації для збільшення безпеки.

5. Авторизація:

•Визначення прав доступу: Надання користувачеві визначених прав доступу до ресурсів системи.

•Контроль доступу: Заходи для обмеження прав доступу відповідно до визначених політик безпеки.

6. Аудит:

•Журналювання: Запис подій та дій для подальшого аналізу та виявлення можливих загроз безпеці.

7. Фізичний захист:

•Обмеження доступу до обладнання: Заходи для запобігання фізичному доступу до інформаційних систем та обладнання.

8. Соціальний інжиніринг:

•Навчання персоналу: Підвищення обізнаності персоналу щодо методів соціального інжинірингу та заходи для запобігання атакам. [9]

Захист інформації є постійним процесом, що включає в себе вдосконалення та адаптацію до нових загроз і технологічних викликів.

Основні аспекти захисту інформації включають технічні, організаційні та правові заходи з метою уникнення ризиків і збереження цінності інформації.

Основними завданнями захисту інформації є:

- виявлення та усунення загроз безпеки нанесенню економічного, фінансового, матеріального та морального збитку;

- створення механізмів реагування на загрози розвитку і функціонуванню підприємства та національній безпеці;

- прийняття заходів щодо забезпечення безпеки персоналу підприємства та інше.

Поняття інформаційної безпеки включає:

- надійність роботи комп’ютера;
- збереження цілісності даних;
- захист інформації від несанкціонованого доступу;
- таємниця електронного листування. [10]

При проведені аналізу проблем, пов'язаної з інформаційною безпекою, потрібно врахувати специфіку даного аспекту безпеки, яка полягає в тому, що інформаційна безпека є складовою частиною інформаційних технологій – області, що удосконалюється високими темпами.

Загалом, під інформаційною безпекою мається на увазі захист документації, відомо, що документ – це матеріальний носій, що містить зафіксовану інформацію, про факти або події. Тому документація в усіх її видах, як в паперовому вигляді так і в електронному обов'язково повинна бути захищеною.

1.2. Особливості організації захисту інформації, документації

Питання організації захисту інформації на даний момент стоїть дуже гостро, адже інформаційні війни ніхто не відміняв, а отже завдяки інформації можемо володіти фінансовими потоками та іншими важливими процесами приватного підприємства. Важливо зазначити, що протягом багатьох попередніх років здійснюються спроби визначити саме сутність поняття «організація». Однак завжди є ряд питань, які залишаються відкритими, дискусійними і потребують подальшого дослідження.

Як поняття організація є комплексом взаємопов'язаних заходів, має особливу єдність із зовнішнім оточенням. Для цього терміну характерним є вираження цілеспрямованого функціонування взаємопов'язаних елементів системи та розвитку.

Організація в широкому розумінні є упорядкуванням усіх елементів системи бухгалтерського обліку, ІТ-сфери, налагодженням і удосконаленням усіх їх процесів.

Система захисту цінної інформації і конфіденційних документів Система захисту інформації (СЗІ) представляє собою комплекс організаційних, технічних і технологічних засобів, методів і мір, які перешкоджають

несанкціонованому (незаконному) доступу до інформації. [11] Тільки комплексна система може дозволити досягненню максимального ефекту захисту інформації, адже системність дає змогу забезпечити необхідні складові й встановлює між ними логічний зв'язок [46].

Важливим й ключовими аспектом в одній із ланок комплексного підходу організації захисту інформації є саме зберігання документації.

Зберігання інформації – забезпечення належного стану інформації та її фізичного носія. Набір заходів, призначених для забезпечення цілісності та цілісності даних, створених шляхом зберігання певної інформації, для створення та підтримки належних умов використання, а також для запобігання несанкціонованому доступу, поширенню та використанню [12]

На рис. 1.3 зображено перелік документів на підприємстві, які мають обов'язково зберігатись.

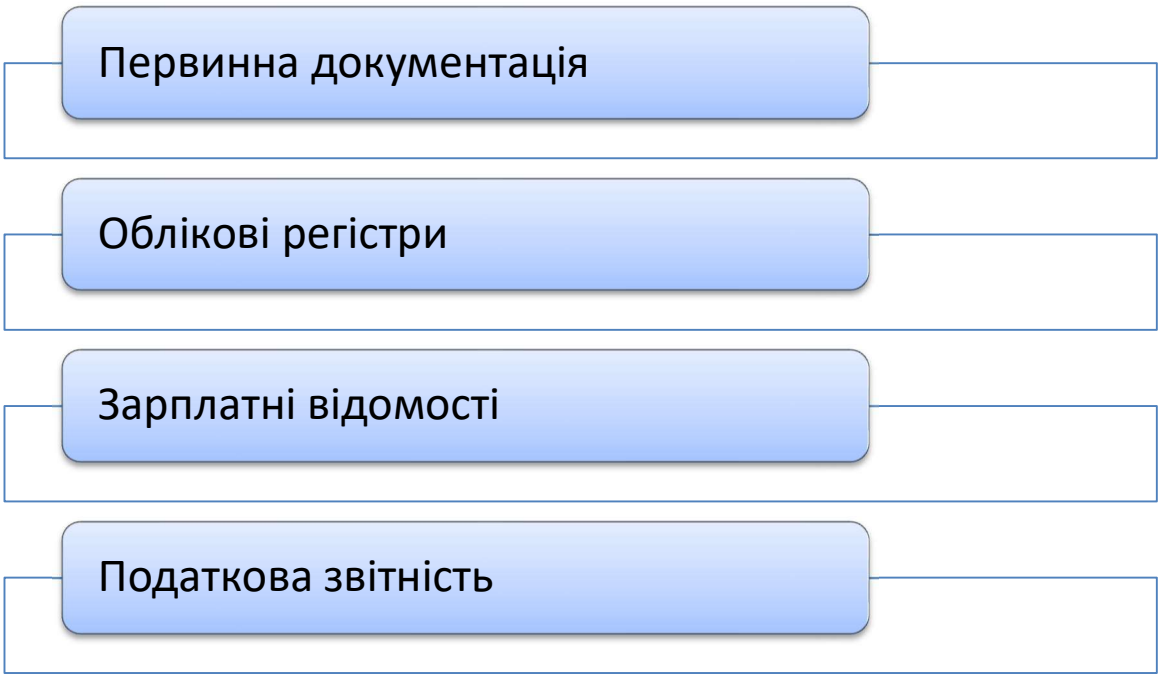

Рисунок 1.3 – Перелік документів обов'язково зберігання

Відповідно до законодавства первинна документація (накладні, чеки, квитанції, акти тощо), облікові регістри, зарплатні відомості (табеля обліку робочого часу), податкова звітність (декларації, розрахунки, відомості, довідки

тощо) мають зберігатися протягом певного строку, а потім знищуватися чи передаватися до архіву.

Терміни зберігання ділової документації визначено Переліком типових документів, що утворюються в діяльності органів державної влади та місцевого самоврядування, інших підприємств, установ та організацій, із зазначенням строків зберігання документів, затвердженим наказом Головного архівного управління при Кабінеті Міністрів України від 20.07.98 р. № 41 (далі – Перелік № 41). Зауважимо, що встановлені цим Переліком терміни є мінімальними, тобто їх не можна скорочувати [14].

Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи [15].

Більшість документів, які підприємство використовує у своїй господарській діяльності, зберігаються три роки. Проте деякі документи потрібно зберігати протягом 5 та навіть 75 років (зокрема, відомості для нарахування зарплати).

Крім того, щодо окремих документів Переліком № 41 передбачені додаткові обмеження. Наприклад, деякі документи можна знищити лише, коли пройдуть перевірку державними податковими органами [16].

Щодо інформації, яка зберігається на електронних носіях.

Усі юридичні особи, підприємства, організації незалежно від форм власності, повинні застосовувати спеціальний Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, затверджений наказом Мін’юсту від 11.11.2014 р. № 1886 [17].

На цей документ слід особливо звернути увагу, адже він містить різноманітні вимоги, зокрема щодо:

· найменування файлів електронних документів;

· найменування файлів електронних облікових документів;

· найменування файлів архівних електронних документів.

Серед іншого установи зобов'язані створювати документи постійного та тривалого (понад 10 років) зберігання у двох формах – паперовій та електронній.

Головною метою будь-якого підприємства чи організації є забезпечення безпеки багатьох інформаційних аспектів.

Основні з них зображені на рисунку 1.4.

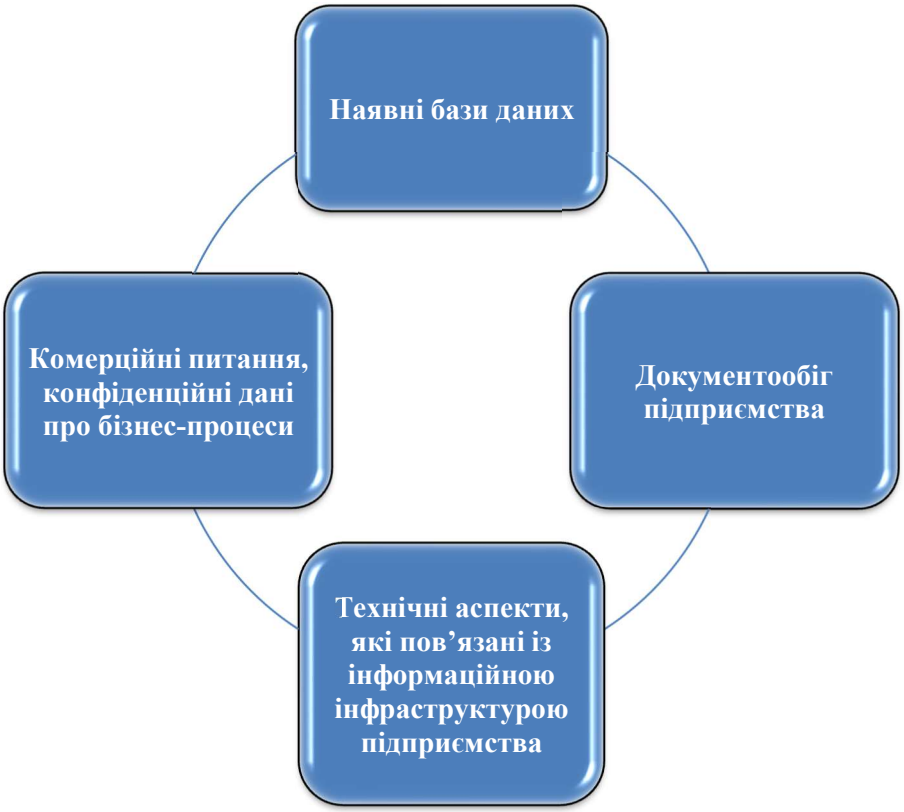

Рисунок 1.4. – Основні аспекти, які потребують захисту інформації

- усіх наявних баз даних, що містять важливі відомості;
- документообіг підприємства, що здійснюється в електронному вигляді;
- різні технічні аспекти, які пов'язані із інформаційною інфраструктурою підприємства;
- комерційні питання, в тому числі конфіденційні дані про бізнес-процеси [18].

Отримання таких відомостей сторонньою організацією, підприємством, державою чи конкретною людною може призвести до серйозних наслідків, навіть до руйнування. Тому дуже важливо мати висококваліфікованих спеціалістів, відповідальних за комплексний захист інформації на підприємстві та її належний контроль.

Електронний захист інформації на підприємстві. Захист інформації на підприємстві має ключове значення для забезпечення безпеки та збереження конфіденційності даних [41].

Розглянемо найефективніші та найпопулярніші заходи захисту, рис. 1.5:

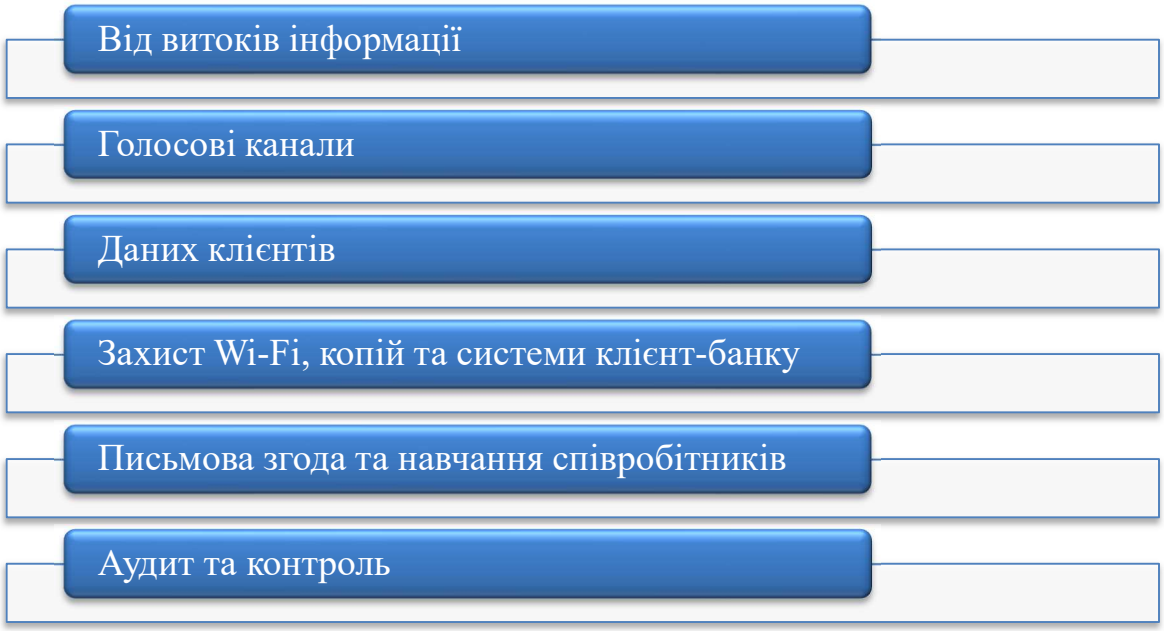

Рисунок 1.5. – Найпопулярніші заходи захисту інформації

•Від витоків інформації. Централізоване зберігання даних. Усі матеріали повинні зберігатися в одному місці, щоб забезпечити контроль за її обробкою та обмежити доступ співробітників до секретних матеріалів. Комплексний підхід до захисту даних допоможе запобігти інфовитіканню через необережність або навмисні дії.

•Голосові канали. Використання IP-телефонії. Встановлення IP-телефонії дозволяє запобігти перехопленню розмов і забезпечити конфіденційність

інформації, що передається телефоном. Це також дозволяє контролювати та записувати всі дзвінки в офісі, що допомагає запобігти витоку секретних матеріалів.

- Даних клієнтів. Інтеграція в програму 1С. Використання програми 1С дозволяє зберігати відомості про клієнтів та автоматично записувати інформацію про дзвінки. Це забезпечує конфіденційність та дозволяє керуючим отримувати доступ до особистих даних клієнтів.
- Захист Wi-Fi, копій та системи клієнт-банку:
  - Wi-Fi-мережа повинна бути захищена, щоб запобігти інфовитоку через уразливі мережі.
  - Регулярне резервне копіювання даних, включаючи віддалене зберігання, дозволяє зберегти інформацію навіть у разі надзвичайних ситуацій чи аварій.
  - Особливу увагу слід приділяти захисту системи клієнт-банку, оскільки це одна з найуразливіших точок доступу для зловмисників.

Крім технічних заходів захисту інформації на підприємстві, існують інші важливі аспекти, які слід врахувати:

- Письмова згода та навчання співробітників. Необхідно отримати письмову згоду від усіх працівників щодо дотримання правил інформаційної безпеки. Регулярне навчання співробітників основ безпеки інформації є невід'ємною частиною захисту даних.
- Аудит та контроль. Адміністратор повинен регулярно проводити аудит системи та контролювати дотримання правил безпеки співробітниками. Це дозволяє виявляти потенційні вразливості та вживати заходів для їх усунення.

Загалом, для забезпечення інфобезпеки малого, середнього та великого бізнесу необхідно вдатися до комплексного підходу. Для цього рекомендується залучення кваліфікованих фахівців, які можуть провести аудит та рекомендувати конкретні заходи захисту з огляду на особливості діяльності компанії.

Використовуючи вищезазначені заходи захисту інформації, підприємства можуть забезпечити надійність та конфіденційність своїх даних, а також запобігти можливим загрозам з боку співробітників та зловмисників.

1.3. Джерела загроз системи захисту інформації

Інформація повинна бути захищено, а для того, щоб розробити етапи потрібно зрозуміти, які ж є джерела загроз інформації. Під загрозою розуміється подія, яка потенційно може порушити одну з властивостей інформації, що захищається. Загрозою ж є будь-які обставини та події, які можуть причинити порушення політики безпеки інформації й нанесення збитку автоматизованій системі [19].

Для сучасних компаній та виробництв основним активним була і залишається інформація. Не тільки унікальні процеси, а й дані про співробітників/клієнтів та зібрана інформація про конкурентів та партнерів є цінною. Будь-яка організація, незалежно від розміру та сфери діяльності, має велику кількість інформації, яка потребує захисту в плані безпеки.

Уразливістю у питаннях інформаційної безпеки є:

1) проблеми, які можуть виникати з комп’ютерним обладнанням чи софтом;
2) несправність поведінки операційних процесів;
3) явні чи приховані недоліки інтерфейсів/протоколів;
4) характеристики систем, що є частиною великої системи;
5) важкі умови експлуатації ПЗ та комп’ютерної техніки;
6) недбалість персоналу/користувачів [20].

Загалом можливі вразливості, які можуть вплинути на інформаційну безпеку, умовно можна розділити на 4 види:

Випадкові. Виникають внаслідок непередбачених обставин та форс-мажорів, пов’язаних із особливостями створеної ІТ-інфраструктури. Це можуть

бути, наприклад, короткочасні збої обладнання через пошкоджені комунікації або знеструмлення офісу.

Об'єктивні. Стосуються конструкції обладнання, що використовується у загальній системі. Також до цього пункту відноситься використання застарілих комплектуючих, несправності, що перманентно виникають, дірки в програмному забезпеченні, вплив перешкод і стрибки напруги.

Намір. Є вторгненням ззовні і виконуються, наприклад, за допомогою активованих «закладок». В їх ролі можуть виступати шкідливі програми, нелегальне ПЗ та інше. До навмисних уразливостей інформаційної безпеки також належить шпигунське обладнання, що використовується для стеження та спору даних.

Виникають внаслідок суб'єктивних чинників. Найчастіше з'являються в результаті помилок користувачів, які виникають в результаті некоректної роботи з ПЗ, файлами, що зберігаються, що знаходяться в доступі та ін. [20]

Таблиця 1.1 – Основні типи вразливості, які можуть вплинути на інформаційну безпеку

№	Вид	Приклад
1	Випадкові	короткочасні збої обладнання через пошкоджені комунікації або знеструмлення офісу
2	Об'єктивні	застарілих комплектуючих, несправності в ПЗ
3	Намір	шпигунське обладнання конкурентів
4	Виникають внаслідок суб'єктивних чинників	помилки користувачів

Найнебезпечнішою вразливістю є навмисна. Від серйозності втручання може залежати не лише інформаційна безпека, а й репутація компанії.

Загрозу можна розглядати як атаку та можливість порушення інформаційної безпеки і посягання на заволодіння інформацією, а той, хто

посягає на інформацію є зловмисником. Загроза проявляються через низький захист або знаходження вразливих місць у системі захисту інформаційних систем [21].

Якщо джерелом загроз є діяльність людини, то говорять про порушника, якщо об'єктивні явища, то говорять про техногенні та стихійні джерела загроз. Поділяють загрози також на: наслідки стихійних лих і техногенних катастроф, відмови обладнання, наслідки помилок персоналу, наслідки помилок системи захисту навмисні дії порушників.

Види загроз, які зазвичай з'являються в результаті небезпечних дій:

- витік даних. Для цього виду загроз об'єктом дій є устаткування (крадіжка носіїв, несанкціоноване використання ресурсів, підключення) програми (перехоплення, несанкціоноване копіювання), дані (копіювання, передача перехоплення), персонал (передача відомостей про захист, розголошення, необізнаність, недбалість);

- порушення цілісності інформації: устаткування (спеціальні вкладення, підключення, зміна режимів, модифікація, несанкціоноване використання ресурсів), програми (впровадження вірусу такого як «троянський кінь» та використання «жучків»), дані (модифікація, спотворення), персонал (вербування, підкуп персоналу);

- порушення роботи системи: устаткування (зміна режимів, виведення з ладу, технічні неполадки, руйнування), програми (спотворення, підміна, вилучення, зміни в роботі), дані (видалення, руйнування, спотворення), персонал (звільнення з посади, байдужість, фізичне усунення).

Можна сказати, що найбільшу загрозу безпеці інформації становлять саме люди, адже саме їхні навмисні чи випадкові не спеціальні дії потрібно передбачати, організовуючи систему захисту.

Співробітники які займаються і працюють у сфері служб комп'ютерної безпеки поділяють усіх порушників на такі чотири групи стосовно жертви:

- сторонні, які не знають компанію;

- сторонні, які знають фірму, та колишні співробітники;

- співробітники-непрограмісти; - співробітники-програмісти.

Людські загрози, зокрема від ненавчених співробітників, можуть становити серйозну загрозу для інформаційної безпеки підприємства. Нижче наведено кілька аспектів, які можуть бути потенційними загрозами:

- Недбалість у використанні паролів:

Співробітники можуть використовувати слабкі паролі або викладати їх непризначеним особам, що збільшує ризик несанкціонованого доступу.

- Неналежне використання технічних ресурсів:

Співробітники можуть намагатися встановлювати неналежне програмне забезпечення або використовувати ресурси підприємства для особистих цілей.

- Небажана передача конфіденційної інформації:

Ненавчені працівники можуть ненавмисно або навмисно розголошувати конфіденційну інформацію поза корпоративним середовищем.

- Несанкціонований доступ до систем:

Недостатня увага до процедур автентифікації та невикористання можливостей безпеки можуть призвести до несанкціонованого доступу до систем.

- Недостатнє навчання з питань інформаційної безпеки:

Якщо співробітники не отримують достатнього навчання з питань безпеки, вони можуть не бути свідомими потенційних загроз та не дотримуватися політик безпеки.

- Використання зовнішніх пристроїв:

Підключення ненадійних зовнішніх пристроїв (USB-накопичувачі, зовнішні жорсткі диски) може відкривати можливості для введення шкідливого програмного забезпечення.

- Недбалість у відносинах з користувачами та вендорами:

Співробітники можуть стати об'єктом соціального інжинірингу та ненавмисно розкривати важливу інформацію під час спілкування з користувачами чи вендорами.

- Неналежна обробка електронної пошти:

Відкриття шкідливих вкладень чи натискання на посилання в електронних листах може призвести до інфікування систем шкідливим програмним забезпеченням.

- Ненавмисна втрата фізичних пристроїв:

Втрата ноутбуків, смартфонів або інших пристроїв може призвести до втрати конфіденційної інформації.

Для зменшення цих загроз важливо регулярно проводити навчання з інформаційної безпеки для всього персоналу, встановлювати строгі політики безпеки та вдосконалювати механізми контролю доступу. Також важливо підтримувати свідомість персоналу щодо загроз і надавати їм засоби для реагування на потенційні інциденти безпеки. Знання потенційних загроз дозволяє вживати превентивних заходів для мінімізації ризиків і запобігання можливим інцидентам безпеки, а також визначити, які засоби та технології захисту будуть найбільш ефективними для запобігання або виявлення атак. Знання і ефективний захист від загроз можуть допомогти запобігти ситуаціям, що можуть завдати шкоди репутації підприємства чи організації, заходи безпеки є обов'язковими для відповідності з законодавством щодо захисту персональних даних та конфіденційної інформації.

1.4. Аналіз ефективної системи захисту інформації на підприємстві

Ефективна система захисту інформації на підприємстві повинна відповідати високим стандартам і вимогам, щоб гарантувати захист важливих даних. Наразі у світі немає єдиної теорії захисту систем; розробники засобів захисту, в основному, пропонують окремі методології для вирішення особистих задач, залишаючи на розсуд споживачів питання формування системи захисту і сумісності цих засобів; для забезпечення надійного захисту необхідно

вирішувати цілий комплекс технічних і організаційних проблем і розробити відповідну документацію.

Аналіз інформаційної безпеки — це процес, покликаний вивчити та оцінити рівень захисту інформаційних систем організації. Його метою є виявлення вразливостей та потенційних загроз безпеці. Послуга дозволяє оцінити ефективність заходів безпеки та надає рекомендації щодо їх поліпшення. [16]

З розвитком технологій та розширенням інтернету, кіберзагрози стають все складнішими та різноманітнішими. Компанії стикаються з ризиками атак хакерів, кіберзлочинності та несанкціонованого доступу до даних. У цій ситуації аналіз інформаційної безпеки стає обов'язковим інструментом для захисту організацій, запобігання кібератакам та мінімізації збитків.

Аналіз інформаційної безпеки включає кілька етапів, таких як збирання інформації про системи, перевірка на вразливості, оцінка ризиків та соціальна інженерія. Кожен із цих етапів відіграє ключову роль у виявленні проблем та наданні рекомендацій для покращення безпеки.

Важливість аналізу інформаційної безпеки

- Виявлення уразливостей. Дозволяє виявити слабкі місця та вразливості в інформаційних системах, які можуть бути використані зловмисниками.
- Оцінка ризиків. Допомагає оцінити потенційні ризики для бізнес-процесів та операційної діяльності компанії.
- Підвищення ефективності захисту. Результати аналізу допомагають удосконалити заходи безпеки для більш ефективної боротьби із загрозами.
- Запобігання інцидентам. Дозволяє виявити потенційні загрози заздалегідь і вжити заходів для запобігання їм.
- Відповідність стандартам безпеки. Гарантує відповідність компанії вимогам безпеки.
- Захист репутації. Допомагає запобігати витоку даних та порушення безпеки, що захищає репутацію компанії [46].

Аналіз інформаційної безпеки стає необхідною складовою стратегії захисту організацій у сучасному цифровому світі. Він допомагає виявити вразливості та застосувати рекомендації для надійного захисту інформаційних систем. Інвестування в аналіз інформаційної безпеки – це важливий крок, який допомагає компаніям зберегти свою репутацію, захистити цінну інформацію та забезпечити успішне функціонування у сучасному конкурентному середовищі.

Переваги аналізу інформаційної безпеки:

По-перше, він дозволяє виявити вразливі місця в інформаційних системах та вжити заходів для їх усунення. Таким чином, компанія стає менш схильна до кібератак і витоків даних, що підвищує загальну безпеку інформації.

По-друге, аналіз інформаційної безпеки допомагає знизити імовірність виникнення інцидентів безпеки. Раннє виявлення потенційних загроз та вжиття відповідних заходів дозволяє запобігти кібератакам або звести їх наслідки до мінімуму.

По-третє, аналіз демонструє турботу компанії щодо безпеки даних своїх клієнтів та партнерів. Це сприяє підвищенню довіри до організації та зміцненню партнерських відносин. [36]

Крім того, проведення аналізу інформаційної безпеки дозволяє компанії відповідати вимогам законодавства та стандартів безпеки. Це особливо важливо для організацій, які працюють з конфіденційною або чутливою інформацією, оскільки це допомагає уникнути штрафів та правових проблем.

Компанія, організація чи підприємство повинні мати політику захисту. Політика захисту – це загальний документ, в якому перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту.

Політика захисту повинна обов’язково включати:

- контроль доступу (заборона на доступ користувача до матеріалів, якими йому не дозволено користуватися);

- ідентифікацію та аутентифікацію (використання паролів або інших механізмів для перевірки статусу користувача);

- ведення обліку (запис усіх дій користувача в мережі);

- контрольний журнал (журнал дозволяє визначити час і місце порушення умов захисту);

- надійність (запобігання монополізації ресурсів системи одним користувачем).

Ключові критерії, за якими слід аналізувати захист інформації на підприємстві і які визначають ефективність системи захисту інформації на підприємстві :

- Конфіденційність:

Шифрування даних: Застосування сучасних методів шифрування для захисту конфіденційної інформації від несанкціонованого доступу.

- Цілісність:

Методи контролю цілісності: Використання контрольних сум, цифрових підписів та інших методів для виявлення будь-яких змін у даних і запобігання їх втраті чи пошкодженню.

- Доступність:

Системи резервного копіювання та відновлення: Існування ефективної стратегії резервного копіювання, яка забезпечує швидке відновлення даних у випадку аварії.

- Аутентифікація та авторизація:

Сильна аутентифікація: Використання багатофакторної аутентифікації для підвищення рівня безпеки при доступі до систем та даних.

- Ефективна система авторизації: Гнучка система керування правами доступу, яка надає права користувачам відповідно до їхніх ролей та обов'язків.

- Моніторинг та виявлення інцидентів:

- Системи моніторингу та аудиту: Забезпечення постійного моніторингу захищених систем для виявлення аномалій та попередження можливих інцидентів.

- Навчання та свідомість користувачів:

Навчання з питань кібербезпеки: Здійснення регулярних навчань та тренінгів для персоналу щодо правил безпеки та управління ризиками.

- Відповідність законодавству:

Впровадження стандартів та вимог безпеки даних: Відповідність до відомих міжнародних стандартів та законодавства, таких як GDPR, HIPAA, ISO 27001.

- Фізична безпека:

Контроль доступу до приміщень та обладнання: Забезпечення безпеки фізичного доступу до серверних приміщень та іншого обладнання.

- Антивірусна та антишпигунська захист:

Використання актуальних засобів захисту: Встановлення та регулярне оновлення антивірусного та антишпигунського програмного забезпечення.

- Системи миттєвого реагування:

Плани безпеки та відновлення: Розробка та впровадження планів дій в разі інциденту для швидкого та ефективного відновлення діяльності.

Ці критерії допомагають забезпечити повноцінний та високий рівень захисту інформації на підприємстві, що є критично важливим в умовах сучасних загроз кібербезпеки.

Аналіз ефективної системи захисту інформації на підприємстві також здійснюється за загальним стандартом, а саме ДСТУ ISO/IEC 27005:2015

Він є найбільш популярним і розповсюдженим на території України. Даний стандарт описує настанови і рекомендується до ознайомлення з метою формування загального уявлення про організацію процесу з управління ризиками

Цей стандарт розглядає стандартні критерії для аналізу ефективного механізму захисту інформації на підприємстві.

Стандартні критерії:

• Критерії зіставлення ризиків;

• Критерії впливу;

• Критерії приймання ризиків.

Оцінка ризиків складається з таких дій:

• Ідентифікація ризику;

• Аналіз ризиків;

• Зіставлення ризиків.

Метою ідентифікації ризику є визначення того, що могло б статися, щоб спричинити потенційні втрати, і щоб отримати уявлення про те, як, де і чому ці втрати можуть виникати.

Етапи, що входять в ідентифікацію ризику, мають збирати вхідну інформацію для дії щодо аналізу ризику:

1. Ідентифікація активів СУІБ (активом є щось, що має цінність для організації і, отже, потребує захисту);

2. Ідентифікація загроз;

3. Ідентифікація існуючих засобів контролю;

4. Ідентифікація вразливостей;

5. Ідентифікація наслідків. Методологія аналізу ризиків може бути якісною чи кількісною, або комбінованою це вже залежно від певних обставин. Рівні ризиків повинні порівнюватися з критеріями оцінювання ризику і критеріями прийняття ризику. Для оцінювання ризиків підприємства виміряні ризики повинні порівнюватися з критеріями оцінювання ризику.

Для обробки ризику є чотири варіанти: модифікація ризику, прийняття ризику, усунення ризику і розподілення ризику.

Одним із таких документів є ще ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. В якому йдеться про те, що організації мають забезпечувати захист своєї інформації й технологічних інфраструктур для збереження бізнесу. Зазвичай це відбувається на ІТ-рівні за допомогою захисту периметра й таких компонентів технологічних структур, як комп’ютери та мережі. Але цього зазвичай недостатньо.

Крім того, організації все більше прагнуть забезпечувати свій захист на рівні корпоративного керування, використовуючи формалізовані, протесговані й перевірені системи керування інформаційною безпекою (СКІБ). Системний

підхід сприяє ефективності систем керування інформаційною безпекою, як описано в ISO/IEC 27001.

Однак у цей час організації стикаються з потребою захисту своєї інформації на рівні додатків, що постійно зростає.

Додатки потребують захисту від вразливостей, які мажуть бути властиві самому додатку (наприклад, дефекти програмного забезпечення), можуть з'являтися протягом життєвого циклу програм (наприклад, в результаті змін додатка) чи виникати в результаті використання додатків за невідповідних умов. Системний підхід до посилення безпеки додатків забезпечує відповідний захист інформації, яку використовують або зберігають додатки організації.

Додатки можуть бути отримані за допомогою внутрішнього розроблення, аутсорсингу чи покупки готового комерційного продукту. Додатки можуть бути також отримані поєднанням підходів, що може призвести до інших наслідків у плані безпеки, які також потребують розгляду та керування.

Прикладами додатків є кадрові системи, фінансові системи, системи обробки текстів, системи керування взаємодією з клієнтами, міжмережеві екрани, антивірусні системи й системи виявлення вторгнень.

Протягом свого життєвого циклу безпечний додаток проявляє необхідні характеристики програмного забезпечення, такі як передбачуване виконання та відповідність, а також виконання вимог щодо безпеки з точки зору розроблення, керування, технологічної інфраструктури та перспективи аудиту.

Для створення надійних додатків, які не збільшують схильності до ризику вище припустимого чи прийнятного рівня залишкового ризику та підтримують ефективну СКІБ, потрібні процеси та практичні прийоми посиленої безпеки, а також кваліфіковані особи для їх виконання.

Крім того, безпечний додаток враховує вимоги щодо безпеки, що випливають з типу даних, цільового середовища (бізнес-контекст, нормативний і технологічний контексти), дійових осіб і специфікацій додатків. Має бути можливість отримання свідчень, які доводять, що припустимий (або прийнятний) рівень залишкового ризику досягнуто та підтримується.

Аналіз інформаційної безпеки відіграє вирішальну роль у захисті інформаційних систем компанії. Це необхідний інструмент для забезпечення надійності та безпеки даних, а також для підтримки довіри клієнтів та партнерів. Інвестування в аналіз інформаційної безпеки є стратегічним рішенням, яке допомагає компаніям бути на крок попереду кіберзагроз та забезпечувати безпечну роботу в сучасних умовах.

Висновки до розділу 1

У першому розділі магістерської роботи було висвітлено теоретичні аспекти захисту інформації, що таке інформація, особливості захисту інформації, джерела загроз системи захисту інформації, аналіз ефективної системи захисту.

Отже, інформація – це знання або дані, які мають сенс або значення для конкретного контексту чи особи. Це може включати в себе факти, ідеї, стан подій, аналіз, спостереження або будь-яку іншу форму опису або висловлювання, які можуть бути використані для розуміння чого-небудь або прийняття рішень. Інформація може бути представлена у різних формах, таких як текст, числа, графіка, звук чи відео, і вона має потенційну вартість для того, хто її отримує та використовує. Важливо, щоб інформація була точною, достовірною та зрозумілою для того, щоб бути корисною та ефективною. Тому захист інформації важливий для усіх типів організацій, оскільки вони опираються на цю інформацію для ефективного функціонування та забезпечення довіри співробітників, партнерів, клієнтів.

Досліджено обов’язковість захисту інформації, захист інформації є дуже кропітким та відповідальним процесом за який несе відповідальність компанія, спеціально відведена особа, а також кожний працівник компанії, який підписував комерційну таємницю.

Визначено особливість захист інформації й актуальність питання у сьогоденні й важливість. Проблема захисту інформації набуває гостроти щоденно, тому до неї потрібно підходити комплексно, робити аналіз, досліджувати проблематику, а також користуватись усіма можливостями реального світу, наймати ІТ професіоналів, юридичних консультантів й інших спеціалістів, які можуть забезпечити Вам або ж вашому підприємству, організації повний захист інформації.

Сучасний бізнес та суспільство не можуть обійтися без інформаційних систем. Вони зберігають, обробляють та передають важливу інформацію, яка визначає стратегічні рішення компаній. Але розвиток технологій також збільшує ризики кібератак та загрози безпеці даних. З вище наведеної інформації також є зрозумілим, що важливо дотримуватись усіх методів захисту інформації, слідкувати і контролювати систему захисту на постійній основі, адже інформаційні технології розвиваються дуже швидко і стрімко розповсюджуються.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ «МАКОШ»

2.1. Загальна характеристика компанії «Макош»: історія створення, розвиток, вид діяльності

Makosh – один з найбільших трейдерів та дистриб'юторів добрив в України. Компанія заснована у 2013 році Поліщуком Віктором Валерійовичем. На сьогодні компанія імпортує понад 150 тис. тон добрив на рік.

Історія компанії Makosh розпочалася ще у 2013 році з ідеї та бажання заснувати сильну та успішну компанію. Віктор Валерійович Поліщук, засновник компанії, розпочинав свій шлях із продажу всього одного продукту – Сульфату Магнію.

Впродовж 3-х років компанія працювала невеличкою командою з 8-ми людей. Поступово бізнес розвивався, а капітал збільшувався. Згодом в асортимент додали NPK добрива. Справжній злет стався у 2014 році, коли було введено ембарго на російські добрива.

У 2013 році, Поліщук Віктор Валерійович втілив новітню систему доставки добрив в Україні. Особливість якої полягала в оплаті за добрива по факту у поєднанні з високим клієнтським сервісом. Цим він поклав початок традиції турботи про фермерів-аграріїв, врожаї та суспільство в цілому. Сьогодні Компанія «Макош» асоціюється з людьми, якістю, надійністю та розвитком. Ми відображаємо цінності Компанії нашим партнерам. Рухаємось і розвиваємось, адже у 2022році відкрили власну компанію у Європі «Makosh Poland». Ми маємо свою культуру бізнесу [22]. Хронологія розвитку розвитку компанії Макош представлена на рис. 2.1.

Рисунок 2.1. – Розвиток (хронологія) компанії Макош

МАКОШ — трейдер та дистриб'ютор мінеральних добрив та добрив для живлення по листу.

Компанія займаємось виключно живлення рослин, це наша мантра, наша релігія для нас важливо бути іконою Клієнтського Сервісу.

МАКОШ – міст між виробником та аграрієм.

Компанія тісно співпрацює із кращими виробниками добрив світу, щоб отримати найкращі добрива, найкращі умови та найкращі ціни для своїх клієнтів

Компанія названа на честь трипільської богині родючості, а знак богині - це знак засіяного поля.

Компанія займаємось виключно живлення рослин, це їх мантра, їх релігія, вони позиціонують себе і для них важливо бути іконою Клієнтського Сервісу.

Слоган компанії «інвестиційне живлення» рослин про те, що всі клієнти це інвестори, тому що добрива купуються для того, щоб отримати кращий урожай та прибуток.

Сьогодні компанія постачає комплексні мінеральні добрива по всій території України вагонами та вантажівками. Вся продукція сертифікована і має міжнародні сертифікати якості та висновки СЕС.

Компанія працює з усіма сільськими господарствами, незалежно від площі полів. Перевагою компанії є індивідуальний підхід до вибору добрив для кожного господарства. Найважливіші аспекти роботи компанії МАКОШ наведено на рис. 2.2.

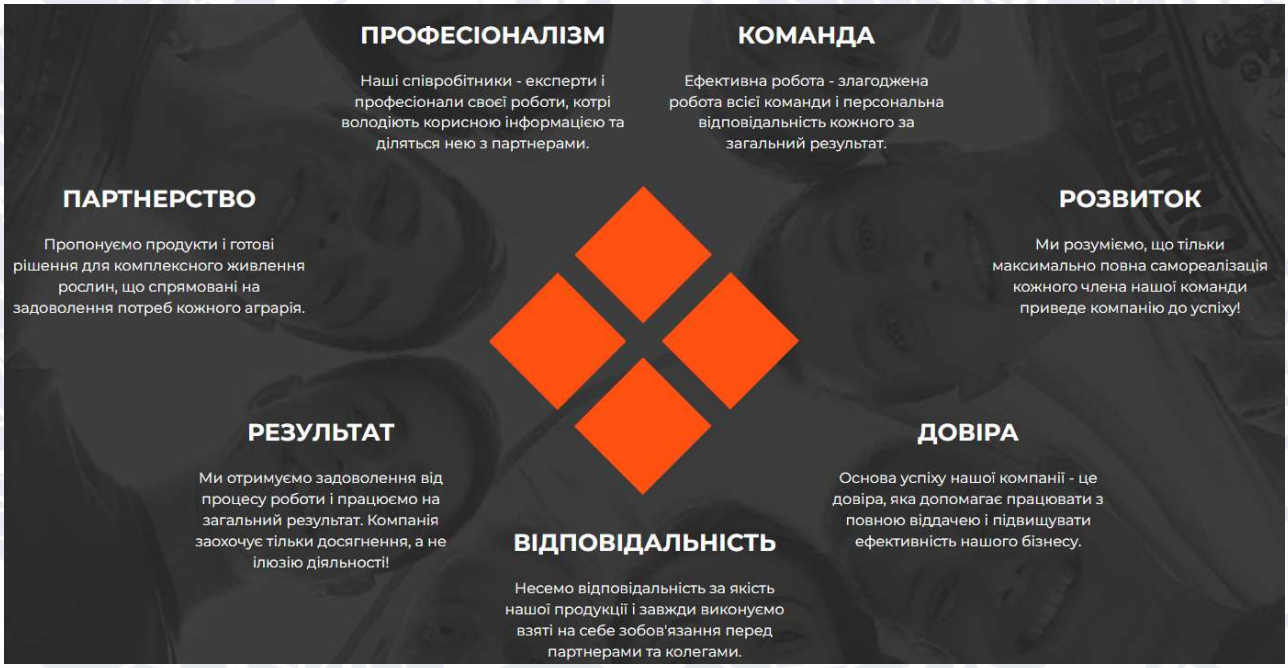

Рисунок 2.2 – Важливі аспекти роботи компанії

МІСІЯ: Ми примножуємо урожай завдяки найкращим технологіям живлення рослин у світі. Створюємо можливості для зростання і процвітання нашої команди.

ФОКУС: Ми займаємось виключно живленням рослин

БАЧЕННЯ: Унікальна компанія, яка динамічно розвивається і досягає всіх задуманих висот. В основі нашого успіху - талановиті колеги, ефективна команда, продукти найвищої якості і кращий сервіс!

ПРИНЦИПИ:

1. Постачаємо тільки ту продукцію, якою ми пишаємось.
2. Партнери - це наші клієнти та постачальники.
3. Піклуємось про наших партнерів.
4. Саме партнери визначають, чи правильно ми рухаємось.
5. Бути відкритим і чесним.
6. Бути щасливим і завжди посміхатись (сміх продовжує життя).
7. Дотримуватись свого слова, завжди!
8. Поважати один одного.
9. Допомагати один одному, ми команда.
10. Успіх компанії - це спільний результат кожного.

Важливим для компанії, яка займається мінеральними добривами це звичайно склади для того, щоб агрономи й фермери могли легко й швидко забрати продукцію. Паралельно з розвитком компанії й купували склади. На рис. 2.3 можна побачити, які ж склади компанія має станом на 2023 рік.

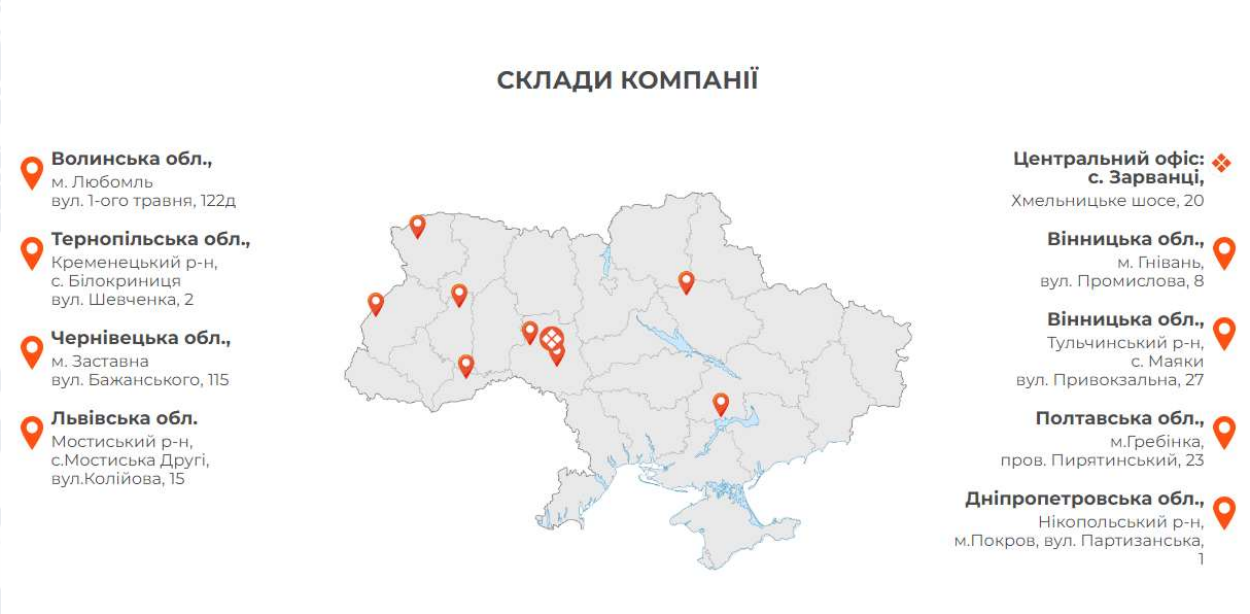

Рисунок 2.3. – Склади компанії, географія складів компанії Макош в Україні

Згодом, компанія розвивалась, бренд став все більш впізнаваним, тому було прийнято рішення найняти професіоналі, а саме дизайнерів для розробки

нового, сучасного логотипу. Тому у 2021 році стався ребрединг і новим кольором компанії став – помаранчевий.

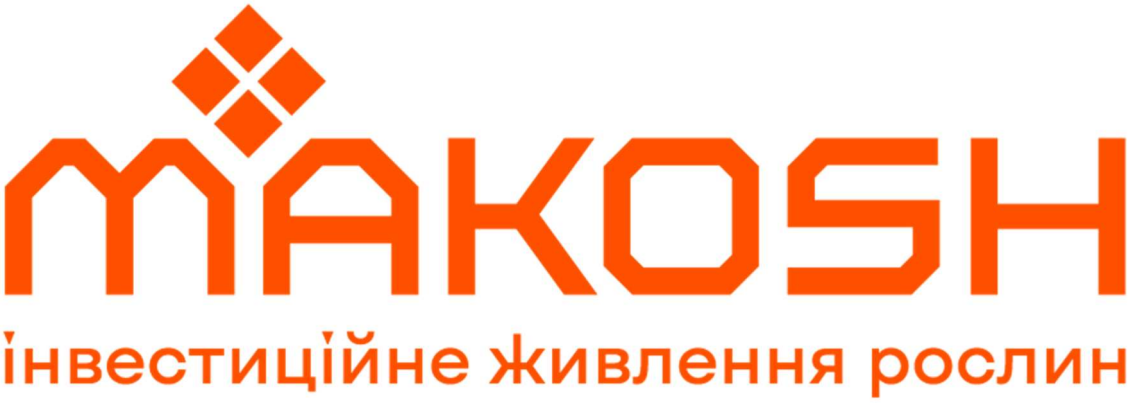

Рисунок 2.4. – Оновлений логотип компанії МАКОШ

Після ребрендингу компанія набула нового етапу, темпу і ритму. Завдяки цьому також компанія почала розвивати й внутрішньо, нові відділи, нові посади, більше людей, робочих місць.

Організаційна структура компанії Макош, відділи, комунікація між ними, правила, традиції.

Прийняття рішень у Макош базується на «раціональності».

Передбачається, що співробітник, який приймає рішення повинен абсолютно об'єктивною і логічно правильно діяти, мати чітку мету, усі його дії в процесі прийняття рішень спрямовані на вибір найкращої альтернативи.

Співробітник, який приймає рішення має:

- мати чітку мету прийняття рішення;
- повну інформацію щодо ситуації для прийняття рішення;
- повну інформацію щодо всіх можливих альтернатив і наслідків їх реалізації;
- раціональну систему впорядкування переваг за ступенем їх важливості.

Мета співробітника, який приймає рішення, завжди полягає у тому, щоб зробити вибір, який максимізує результат діяльності компанії

У Макош усі співробітники:

«Наші найкращі люди не просто відповідають Культурі, вони сприяють її розвитку»!

1. Відповідають корпоративній культурі та її дотримуються:
2. Постійно вдосконалюються і навчаються
3. Ініціюють та втілюють зміни
4. Прагнуть до перемог і лідерства

Норми і правила.

Розроблені «правила утримання і поводження в офісному приміщенні Макош та на прилеглій території» наголошують на необхідності та обов'язковості їх дотримання усіма співробітниками компанії, наведені нижче:

ІНФОРМАЦІЙНА БЕЗПЕКА

Інформація, котра знаходиться у CRM-системі, 1С, базі знань, гул-диску, на пошті, в робочих ПК та телефонах (у тому числі контакти, інформація з чатів) – є Конфіденційною!

Заборонено передавати доступи та інформацію третім особам!

А також інші правила такі, як правила поводження в офісі, тренажерним залом, тенісним кортом, прилеглою територією.

Цікавим є інформація, щодо традицій і звичаїв.

У Макош ми створюємо атмосферу, яка формує клімат Компанії.

Кожен працівник знає, що його «інвестиції» цінують та поважають.

Наші сформовані традиції і звичаї є невід'ємною складовою корпоративної культури, яка підвищує лояльність та залученість працівників.

Лояльна команда працює на результат, вона зацікавлена у розвитку. [2]

Це про повагу до людей, з якими нас об'єднує спільна мета.

В компанії функціонують такі відділи рис. 2.5:

- операційний в який входить (HR відділ);
- IT;
- відділ продажу, до якого входить (маркетинг, аудит грунту);
- бухгалтерія;

- фінансовий відділ;
- логістика;
- відділ розвитку й контролю;
- адміністративно господарський відділ.

Рисунок 2.5 – Організаційна структура компанії «Макош»

Отож, компанія Макош на сьогодні налічує близько 160 співробітників, має працівників у віддаленому форматі, а також складські приміщення по Україні, які не мають повного контролю, як наприклад у головному офісі. Компанія, яка займається мінеральним добривами є конкурентною, постійний потік кадрів, що провокує більший витік інформації, систему роботи, та інші конфіденційні моменти внутрішньої діяльності. Тому дуже важливо вміло організувати систему захисту інформації, сформувати чіткий план дій, назначити відповідальних за контроль захисту інформації.

2.2. Аналіз проблем організації захисту інформації на досліджуваному підприємстві

Кожне підприємство чи організація, будь-якого типу чи державної чи приватної власності, має свої проблеми та недоліки. Тому, завжди дуже важливо вчасно їх виявити та вчасно ліквідувати й організувати правильне, чітке рішення для покращення тих чи інший процесів, систем діяльності компанії.

На підприємствах існує безліч потенційних проблем у сфері захисту інформації. Розглянемо деякі з найбільш поширених проблем:

1. Невідповідний рівень свідомості:

Співробітники: Брак свідомості та недостатнє навчання серед працівників може сприяти виникненню загроз безпеці. Наприклад, не усвідомленість про соціальні інженерні атаки або погані практики парольної безпеки.

2. Недостатня фізична безпека:

Доступ до обладнання: Недостатній контроль за доступом до серверних приміщень або інших пристроїв може призвести до незаконного доступу до конфіденційної інформації.

3. Не відповідна мережева безпека:

Несанкціоновані доступи: Недостатній захист мережі може стати причиною несанкціонованих доступів до інформації або витоків даних.

4. Неналежна безпека програмного забезпечення:

Вразливості систем: Використання застарілих програм або вразливостей у програмному забезпеченні може дозволити зловмисникам отримати доступ та контроль над системами.

5. Відсутність ефективного моніторингу:

Недостатній аудит: Не ведеться ефективний моніторинг подій у системах, що може призвести до затримок у виявленні і реагуванні на потенційні загрози.

6. Неефективна політика паролів:

Слабкі паролі: Використання слабких паролів або відсутність політики щодо їх регулярної зміни може зробити системи вразливими.

7. Загрози зсередини:

Несанкціоновані дії працівників: Дії чи недбалість власних працівників можуть стати внутрішньою загрозою для інформаційної безпеки.

8. Недостатній рівень шифрування:

Нешифрована інформація: Недостатнє застосування шифрування може призвести до можливості перехоплення конфіденційної інформації.

9. Відсутність плану відновлення після інциденту:

Відновлення після кризи: Відсутність плану відновлення та резервного копіювання може ускладнити відновлення даних після інциденту безпеки.

10. Застосування застарілих технологій:

Не підтримка виробником: Застосування застарілих технологій, які не отримують поновлень безпеки від виробників, може збільшити ризик [23].

Для вирішення цих проблем рекомендується впровадження комплексної політики інформаційної безпеки, регулярне оновлення програмного та апаратного забезпечення, навчання персоналу та ведення систематичного моніторингу безпеки.

Згідно з цією інформацію, було прийнято рішення провести інтерв'ю з керівниками відділів та провести аналіз проблематики в досліджуваній мною компанії «Макош». Керівники відділів, а саме керівники відділів, які займаються підбором персоналу, проводять навчання, займаються веденням бухгалтерії й звичайно технічним забезпечення компанії – це HR-директор, головний бухгалтер та керівнику відділу IT.

Було задано наступний ряд запитань:

1. Які конкретні заходи захисту інформації вже впроваджені в компанії?
2. Чи проводилися оцінки ризиків щодо захисту інформації в останній часі? Якщо так, які результати були отримані?
3. Які види конфіденційної інформації обробляються в компанії, і як вони захищені?
4. Чи існують навчальні програми для співробітників з питань безпеки та захисту інформації?
5. Як часто проводяться аудити безпеки для перевірки ефективності захисту інформації?
6. Чи існують плани невідкладних заходів в разі порушення безпеки чи витоку інформації?
7. Чи залучені зовнішні експерти для перевірки та підтримки систем безпеки?

За проведенням усного інтерв’ю з керівниками відділів було виявлену вузькі місця діяльності команди й компанії в цілому у організації захисту інформації. А саме, щодо конкретних заходів захисту інформації, чітких й структурованих заходів не існує, окрім створення комерційної таємниці, яка підписується кожним новим співробітником, а також компанія забезпечує кожного працівника магнітною карткою для зберігання секретного ключа, за допомогою якого вони можуть зайти в офіс, цим передбачено контроль перебування сторонніх осіб. А також територія офісної будівлі оснащена системою відеоспостереження та відеореєстрації, що дають змогу вести цілодобовий візуальний нагляд як за периметром об'єкта, так і всередині з можливістю запису інформації на комп'ютер. Одним із методів інформаційної безпеки у компанії є попередження від адміністраторів ІТ-відділу про фітингові атаки чи нові шахрайські схеми (додаток А). Оцінка ризиків щодо захисту інформації в компанії не проводилась. Конкретні види інформації, які зберігаються на підприємстві: персональні інформація (особисті дані співробітників, клієнтів), бізнес-інформація (стратегічні плани, фінансові звіти, угоди, контракти), інтелектуальна власність (дизайн, ідеї), комерційна інформація (плани, дані, стратегії ціноутворення), конфіденційні операційні дані (постачальники, дані виробничих процесів), зовнішня документація (юридичні документи, угоди, судові матеріали). Навчальних процедур не існує, при адаптації нового співробітника проговорюється важливість конфіденційності інформації. Аудит безпеки для перевірки ефективності захисту інформації не проводиться, а також немає плану невідкладних заходів в разі порушення безпеки й витоку інформації, не залучено зовнішні експертів для створення системи безпеки.

2.3 Взаємозв’язок організації системи захисту інформації з ефективною діяльності підприємства

Взаємозв'язок організації системи захисту інформації з ефективною діяльністю підприємства є критично важливим у сучасному світі, де інформація вважається одним із ключових активів будь-якої організації. Загальною тенденцією є те, що захист інформації стає невід'ємною частиною стратегії керівництва підприємства, і недостатність заходів у цьому напрямку може призвести до серйозних наслідків для бізнесу.

Організація системи захисту інформації впливає на різні аспекти діяльності підприємства, які наведені на рис. 2.6.

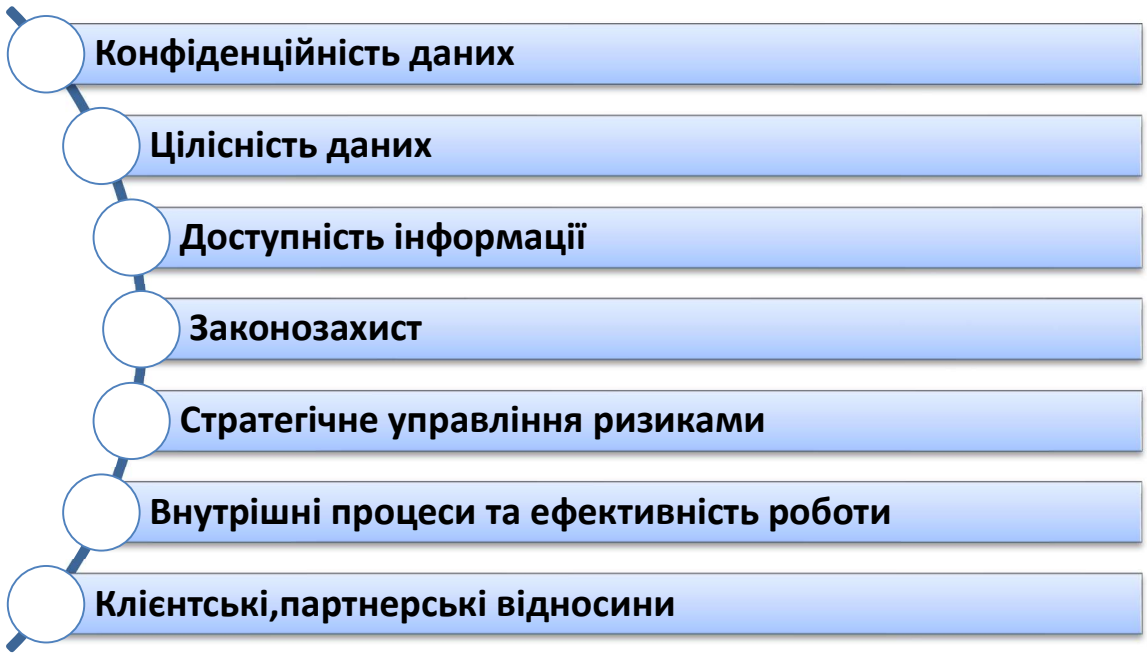

Рисунок 2.6 – Основні аспекти діяльності підприємства на які має вплив захист інформації

1. Конфіденційність даних:

Організаційний успіх: Захищена від несанкціонованого доступу інформація гарантує, що конфіденційна та стратегічна інформація підприємства залишається в безпеці. Це може бути важливим фактором успіху в конкурентному середовищі.

2. Цілісність даних:

Якість продукції та послуг: Захищена від змін інформація гарантує цілісність бізнес-процесів, що впливає на якість продукції та послуг, які надає підприємство.

3. Доступність інформації:

Продуктивність та ефективність: Забезпечення доступності до інформації в потрібний момент є ключовим для продуктивності та ефективності операцій підприємства. Заходи зі збереження доступності інформації можуть включати резервне копіювання, відновлення після збоїв тощо.

4. Законозахист:

Уникнення штрафів та репутаційних втрат: Захист інформації відповідно до законодавства допомагає уникнути штрафів та інших юридичних наслідків, що можуть вплинути на репутацію підприємства.

5. Стратегічне управління ризиками:

Стійкість до кіберзагроз: Посилення заходів з захисту інформації допомагає підприємствам бути більш стійкими до кіберзагроз, що є актуальною проблемою у сучасному світі.

6. Внутрішні процеси та ефективність роботи:

Ефективне управління інформацією: Захищена система дозволяє підприємству ефективно управляти своєю інформацією, впливаючи на внутрішні процеси та сприяючи прийняттю правильних управлінських рішень.

7. Клієнтські, партнерські відносини:

Довіра клієнтів: Захист персональних даних клієнтів впливає на рівень довіри, що має ключове значення для відносин з клієнтами.

Загалом, впорядкована та ефективна система захисту інформації не лише забезпечує безпеку, а й виступає як стратегічний актив, сприяючи узгодженому та ефективному функціонуванню підприємства [24].

Важливим аспектом є те, що не усі працівники компанії є добросовісними, а мають на меті використовувати дані компанії на свою вигоду (це може бути розповсюдженість інформації конкурентам, або ж вивчення внутрішньої діяльності компанії для навичок створення своєї). Це породжує нездорову

конкуренцію, витік інформації, який впливає на прибутковість даної компанії, репутацію (негативні наслідки витоку чи незаконного використання інформації можуть призвести до серйозної втрати репутації підприємства в очах клієнтів, партнерів та громадськості). Законодавство України закріплює, що відповідальність за порушення законодавства про інформацію є гарантією права на інформацію і полягає у притягненні до дисциплінарної, цивільно-правової, адміністративної та кримінальної відповідальності.

Компанія Макош складається з 160+ працівників, а саме офісних та складських, тому важливим моментом є захист інформації та документації. Попередньо прописуючи правила компанії, вже згадувалось про конфіденційність інформації. Створено окремий документ, який є важливим аби працювати в команді. Документ, який має назву: «Перелік відомостей, що становлять комерційну таємницю Компанії «МАКОШ» містить в собі наступну інформацію.

До інформації, що є конфіденційною і складає комерційну таємницю ТОВ «МАКОШ МІНЕРАЛ» відносяться дані, які наведені на рисунку 2.7.

Рисунок 2.7 – Основні дані, які є конфіденційним на підприємстві МАКОШ

1. Управління підприємством.

Відомості про:

1.1 Способи та засоби управління підприємством;

1.2 Підготовку, прийняття та виконання окремих рішень керівництва підприємства з комерційних, організаційних, виробничих, та інших питань.

2. Плани підприємства.

Відомості про:

2.1. Плани розширення/ згортання виробництва, продажу та техніко-економічне обґрунтування;

2.2. Плани закупівель, продажу та інвестицій.

3. Наради.

Відомості про факти проведення, цілі, предмет та результати нарад органів управління підприємством.

4. Фінанси підприємства.

Відомості про:

4.1 Рух грошових коштів по рахунках підприємства;

4.2 Про залишки на рахунках;

4.3 Бюджет доходів та витрат підприємства;

4.4 Банківські зв’язки;

4.5 Відомості, які розкривають плани і фактичні показники фінансового стану.

5. Партнери підприємства.

Узагальнені відомості про постачальників, клієнтів, виконавців, покупців та інших суб’єктів, що є сторонами діючих договорів, угод, зовнішньоекономічних контрактів Підприємства щодо експорту, імпорту, реалізації на внутрішньому ринку товарів робіт чи послуг, у т.ч. відомості про фінансовий стан, репутацію та інші дані, що характеризують ступінь надійності партнера або його представників, якщо їх розголошення може завдати збитків Підприємству, за винятком якщо розповсюдження частини цієї інформації необхідно для здійснення закупівельної діяльності або прийняття рішення щодо

можливості співпрацювання з вказаним(и) постачальником, замовником, продавцем, виробником, виконавцем, покупцем та інших.

6. Контракти.

Відомості про:

6.1) умови за контрактами, угодами як укладеними, так і тими, які плануються (строки, об'єми, номенклатура, умови поставки);

6.2) особливі умови контрактів (скидки, доплати, розстрочки платежів, опції);

6.3) умови платежів по контрактам (скидки, доплати, розстрочки платежі, опції);

6.4) особливі угоди і умови компенсаційних угод;

6.5) відомості про виконання контрактів:

6.6) відомості про номенклатуру і кількість товарів за взаємними зобов'язаннями, передбаченими угодами, протоколами, а також про товарообіг.

7. Ціни та ціноутворення.

Відомості про:

7.1) методику розрахунку цін і принципи ціноутворення;

7.2) структуру цін;

7.3) структуру продажної калькуляції;

7.4) калькуляцію витрат виробництва;

7.5) собівартість продукції;

7.6) розмір торгової націнки;

7.7) дані для калькуляції ціни.

8. Виробництво.

Відомості про:

8.1) виробничі потужності;

8.2) виробниче обладнання;

8.3) запаси сировини, матеріалів, комплектуючих і готової продукції;

8.4) поточні і перспективні плани виробництва; стратегію виробництва;

8.5) постачальників, продавців та покупців підприємства;

8.6) способи придбання та реалізації продукції підприємства.

9. Інформаційні дані.

9.1. Дані, що містяться у базах даних Підприємства, 1С, CRM, WizzyLab, тощо.

9.2. Відомості про бази даних (число користувачів, загальний обсяг дискового простору, який займає база даних, модулі програмного продукту тощо), комп'ютерні програми, створені на Підприємстві.

9.3. Паролі до адміністративних, технологічних та персональних облікових записів, у т.ч. паролі доступу до корпоративних точок WiFi, внутрішньої мережі, корпоративного сайту, корпоративних сторінок у соціальних мережах, електронної пошти, баз даних Підприємства.

9.4. Матеріали системи відеоспостереження, дані про переміщення працівників по приміщеннях Підприємства, зафіксовані електронною системою контролю доступу

9.5. Дані про схему, конфігурацію апаратних засобів, серверів, системи відеоспостереження та системи електроживлення внутрішньої мережі Підприємства.

9.6. Дані, що містяться у месенджерах (Telegram, Viber), корпоративній пошті, а також Trello й інші мережі та додатки, які ви використовували для передачі робочої інформації.

А також важливим документом, який підписує кожний з нових працівників є зобов'язання, щодо нерозголошення інформації, що становить комерційну таємницю Компанії «Макош». Яке зобов'язує на період трудових відносин з ТОВ «Макош Мінерал» (надалі – Підприємство) та упродовж 5 (п'яти) років після їх завершення:

1. Не передавати третім особам, не розкривати публічно та не розголошувати відомості, що становлять конфіденційну інформацію та комерційну таємницю Підприємства, які можуть бути довірені мені або стануть відомі під час виконання трудових обов'язків.

2. Чітко виконувати вимоги Положення про комерційну таємницю та конфіденційну інформацію ТОВ «Макош Мінерал».

3. Не використовувати інформацію, що становить конфіденційну інформацію або комерційну таємницю, для зайняття будь-якою діяльністю, що може завдати шкоди інтересам Підприємства в якості конкурентної діяльності.

4. Терміново повідомляти безпосередньому керівнику про випадки втрати паперових, електронних, магнітних носіїв конфіденційної інформації або комерційної таємниці, посвідчень, перепусток, ключів від приміщень та сейфів, печаток та штампів Підприємства.

При спробі сторонніх осіб отримати відомості, що становлять конфіденційну інформацію або комерційну таємницю уникати їх розголошення та негайно повідомляти про це керівних осіб Підприємства.

Порушення умов про нерозголошення комерційної таємниці Підприємства може тягнути за собою притягнення до кримінальної, дисциплінарної (в тому числі і звільнення), цивільно-правової та іншого виду відповідальності згідно з чинним законодавством України.

У документі наведено зміст статей 231, 232 Кримінального кодексу України та ст. 164^3 Кодексу України про адміністративні правопорушення для ознайомлення й попередження усіх співробітників .

Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю

Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, - караються штрафом від трьох тисяч до восьми тисяч неоподатковуваних мінімумів доходів громадян [25].

Стаття 232. Розголошення комерційної або банківської таємниці

Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або

службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років [26].

Стаття 164^3. Недобросовісна конкуренція

Незаконне копіювання форми, упаковки, зовнішнього оформлення, а так само імітація, копіювання, пряме відтворення товару іншого підприємця, самовільне використання його імені тягне за собою накладення штрафу від тридцяти до сорока чотирьох неоподатковуваних мінімумів доходів громадян з конфіскацією виготовленої продукції, знарядь виробництва і сировини чи без такої.

Умисне поширення неправдивих або неточних відомостей, які можуть завдати шкоди діловій репутації або майновим інтересам іншого підприємця, - тягне за собою накладення штрафу від п'яти до дев'яти неоподатковуваних мінімумів доходів громадян [27].

Отримання, використання, розголошення комерційної таємниці, а також іншої конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця - тягне за собою накладення штрафу від дев'яти до вісімнадцяти неоподатковуваних мінімумів доходів громадян».

Підприємство підтверджує, що дані Вами зобов'язання не обмежують Ваших прав на інтелектуальну власність.

Висновки до розділу 2

У розділі 2 магістерської кваліфікаційної роботи автором було розглянуто загальну характеристику обраного підприємства компанії «Макош», проведено аналіз проблеми організації захисту інформації на підприємствах, досліджено

взаємозв’язок організації системи захисту з ефективною діяльністю компанії в цілому.

Визначено, що компанія - це організаційна одиниця, яка діє в економічній системі з метою виробництва товарів або надання послуг. Компанія може мати різні форми власності, структури та розміри, а також функціонувати в різних галузях економіки. Вона об'єднує групу людей, ресурси та технології для досягнення певної мети та отримання прибутку. Будь яка компанія, організація, державна структура повинні організувати захист інформації для документації.

Проаналізовано, що на підприємствах є безліч проблем, а також і у сфері захисту інформації. Такі як: невідповідний рівень свідомості, недостатня фізична безпека, не відповідна мережева безпека, неналежна безпека програмного забезпечення, відсутність ефективного моніторингу,неефективна політика паролів, загрози зсередини, недостатній рівень шифрування, відсутність плану відновлення після інциденту, застосування застарілих технологій.

Здійснено особисте, усне інтерв’ю із керівниками HR-відділу, IT-відділу та бухгалтерського відділу аби дослідити внутрішні проблеми захисту інформації на підприємстві, а саме у відділах. Було задано ряд питань, де дослідити декілька очевидних проблем організації захисту інформації у компанії «Макош».

Встановлено, що на підприємстві практично немає механізму захисту інформації, що дане питання піднімається дуже рідко, що нові співробітники компанії необізнані у конфіденційної інформації, у технічному забезпечені, а також немає закріпленої особи, яка веде усю кадрову діяльність даної компанії.

Існуючий механізм захисту у компанії «Макош» є недосконалим, та потребує кардинальних змін, яким можна досягти шляхом розробки механізмі, що автоматизують деякі процеси та забезпечать захист документації.

РОЗДІЛ 3
МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЇ ТА ДОКУМЕНТАЦІЇ НА ПІДПРИЄМСТВІ

3.1. Методи удосконалення системи захисту інформації у компанії «Макош»

Призначення системи інформаційної безпеки полягає в організації безпечних і надійних: заходів з доступу до інформації, способів передачі та зберігання інформації, методів обробки інформації, правил управління доступом до інформації, способів відновлення інформації, методів резервування інформації тощо.

Удосконалення системи захисту інформації – це невід'ємна частина стратегії кібербезпеки організації чи компанії. Створюючи системи захисту на підприємстві, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв’язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це значить, що засоби захисту інформації мають застосовуватися одночасно і під централізованим управлінням. При цьому усі компоненти системи мають розуміти і знати про існування один одного, взаємодіяти і забезпечувати захист від усіх і зовнішніх і від внутрішніх загроз. Тобто,

систему захисту інформації потрібно налагодити таким чином, аби кожний розумів свою цінність в її організації і її захисту.

Для забезпечення захисту інформаційного середовища підприємства необхідне систематичне виконання наступних етапів (рис. 3.1):

- аналіз загроз інформаційній безпеці; (рис. 3.2):

- планування та розробка заходів щодо забезпечення інформаційної безпеки;

- оперативна реалізація запланованих дій [28].

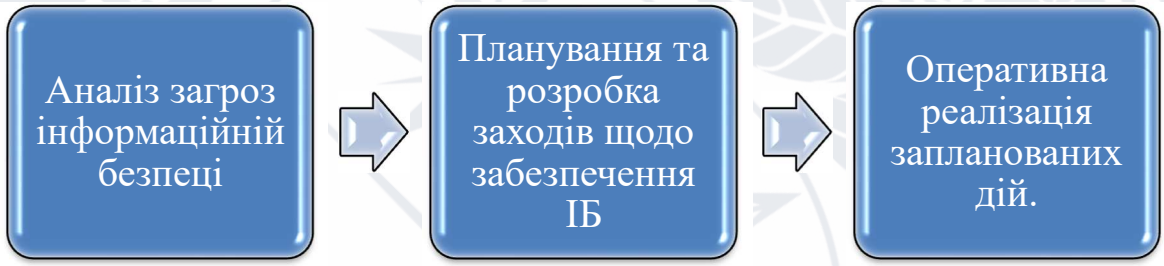

Рисунок 3.1 – Етапи для систематичності захисту інформації

Головною метою підприємства є забезпечення безпеки саме таких аспектів:

- усіх наявних баз даних, що містять важливі відомості;
- документообіг підприємства, що здійснюється в електронному вигляді;
- різні технічні аспекти, які пов'язані із інформаційною інфраструктурою підприємства;
- комерційні питання, в тому числі конфіденційні дані про бізнес-процеси [44].

Повстає питання, які ж є джерела спотворення й загроза інформації. Загрозою ж є будь-які обставини та події, які можуть причинити порушення політики безпеки інформації й нанесення збитку автоматизованій системі. [45]

Поділяють загрози: наслідки стихійних лих і техногенних катастроф, відмови обладнання, наслідки помилок персоналу, наслідки помилок системи захисту навмисні дії порушників. Детально наведено на рис. 3.2.

Класифікація загроз знищення інформації:

Рисунок 3.2 – Класифікація загроз знищення інформації

- Наслідки стихійних лих і техногенних катастроф – методи боротьби це резервування апаратного забезпечення, резервні копії.

- Відмови обладнання – методи боротьби це резервування, копії, вибір надійного постачальника апаратного забезпечення.

- Наслідки помилок персоналу – методи боротьби ретельне підбирання персоналу, навчання, створення систем адміністративних стягнень за порушення, створення позитивної атмосфери у середині колективу.

- Наслідки помилок системи захисту – методи боротьби це залучення ліцензованих спеціалістів, експертиза проекту, періодичний аудит системи захисту.

- Навмисні дії порушників – методи боротьби зазвичай залежать від способу дій [29].

У теорії доведено, якщо система захисту інформації побудована за попередньо описаною схемою, то частіше за все навмисні дії порушників у такій системі неможливі. Але все ж жодна з систем захисту не дає гарантії й не може довгий час протидіяти цілеспрямованим діям сучасних технологій, а особливо, коли діє кваліфікований порушник [30].

Виділяють наступні основні методи експертних оцінок, що застосовуються для аналізу небезпеки: запитальники; SWOT-аналіз; роза і спіраль ризиків; оцінка ризику стадії проекту; метод Дельфі.

Метою системи захисту інформації підприємства є:

- запобігання витоку даних, втраті, розкраданню, перекручуванню, підробці інформації;
- запобігання загрозам безпеці особистості, підприємства, суспільства, держави;
- запобігання несанкціонованим діям щодо знищення, модифікації, перекручування, копіювання, блокування інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси й системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, що існують в інформаційних системах;
- збереження конфіденційності документованої інформації відповідно до законодавства.

Для грамотної побудови й експлуатації системи захисту необхідно дотримуватись таких принципів її застосування:

- простота захисту;
- прийнятність захисту для користувачів;
- підконтрольність системи захисту;
- постійний контроль за найбільш важливою інформацією;

•дроблення конфіденційної інформації на складові елементи, доступ до яких мають різні користувачі;

•мінімізація привілеїв доступу до інформації;

•установка пасток для провокування несанкціонованих дій;

•незалежність системи керування для користувачів;

•стійкість захисту в часі й за несприятливих обставин;

•глибина захисту, його дублювання й перекриття;

•особлива персональна відповідальність осіб, що забезпечують безпеку інформації;

•мінімізація загальних механізмів захисту.

Порядок створення системи захисту конфіденційної інформації (рис. 3.3) такий:

Рисунок 3.3 – Порядок створення системи захисту конфіденційної інформації

•визначення об'єктів захисту;

•виявлення загроз і оцінка їхньої ймовірності;

•оцінка можливої шкоди;

•огляд застосовуваних засобів захисту, визначення їхньої недостатності;

- визначення адекватних заходів захисту;
- організаційне, фінансове, юридичне та ін. види забезпечення засобів захисту;
- впровадження засобів захисту;
- контроль;
- моніторинг і коригування впроваджених засобів

Інформаційна безпека досягається впровадженням необхідного набору заходів безпеки, які можуть включати політики, інструкції, директиви, організаційні структури та можливості програмного забезпечення. Ці інструменти повинні бути реалізовані, щоб забезпечити виконання вимог безпеки конкретної організації.

Інформація може існувати в багатьох формах. Він може бути надрукований або написаний на папері, збережений на електронних носіях, пересланий традиційним або електронним листом, представлений у вигляді фільму або переданий у вигляді усної розмови. Незалежно від того, яку форму приймає інформація або як вона передається та зберігається, завжди необхідно забезпечити відповідний рівень захисту.

3.2. Механізм захисту інформації та документації у компанії «Макош»

Для компаній надзвичайно важливо не лише розглядати інциденти, які вже відбулися, але й створювати засоби захисту, які можуть протистояти атакам до виникнення проблем і навіть до виявлення потенційних проблем і вразливостей.

Для забезпечення ефективності розробленої системи захисту інформації необхідно створити в організації спеціальний відділ, який займатиметься цими питаннями – служби захисту інформації.

1. Відповідальний за службу захисту інформації призначається наказом керівника підприємства. Він очолює групу досвідчених співробітників, які надають консультації щодо обсягу, рівня та методів забезпечення збереження конфіденційної інформації.

2. Керівник групи з відповідною кваліфікацією в галузі за участю окремих експертів формує попередній перелік відомостей, які в подальшому включають до «переліку відомостей, що становлять конфіденційну корпоративну інформацію».

3. Керівник групи визначає за переліком об’єкти, які потребують охорони, та подає їх на затвердження.

4. Проаналізувати наявні засоби захисту суб’єкта та визначити ступінь їх неадекватності, неефективності, фізичної та психічної зношеності.

5. Дослідити задокументовані факти спроб несанкціонованого доступу до захищених інформаційних ресурсів та витоку інформації.

6. Виходячи з досвіду компанії, експертна група використовує методи ситуаційного моделювання для виявлення можливих несанкціонованих дій щодо знищення інформації, копіювання інформації, модифікації інформації, спотворення інформації, використання інформації тощо. Загрози впорядковано за ступенем серйозності та класифіковано за типом впливу.

7. На основі зібраних даних оцініть можливу шкоду, завдану підприємству різними загрозами, що стає вирішальним фактором у класифікації інформації у «списку» за її важливістю, наприклад, для службового користування, конфіденційної та суворо конфіденційної. .

8. Обсяг обігу кожного виду конфіденційної інформації визначається носіями, зоною поширення та дозволеними користувачами. Для вирішення цього завдання група запросила керівників структурних підрозділів вивчити їхні побажання.

9. Організація готується до впровадження спеціальних засобів захисту[39].

До завдань Служби захисту інформації належить:

- своєчасне виявлення загроз інформації, яка захищається, причин і умов їхнього виникнення й реалізації;
- виявлення й максимальне перекриття потенційно можливих каналів і методів несанкціонованого доступу до інформації;
- відпрацьовування механізмів оперативного реагування на загрози, використання юридичних, економічних, організаційних, соціально-психологічних, інженерно-технічних засобів і методів виявлення й нейтралізації джерел загроз безпеці компанії;
- організація спеціального діловодства, що виключає несанкціоноване одержання конфіденційної інформації.

Начальник Служби захисту інформації – новий службовий підрозділ. На дану посаду має прийти професійний фахівець у сфері захисту інформації, який знає юридичні аспекти питання та має досвід управління та координації роботи подібних служб. Вимоги: мати вищу професійну освіту не менше 5 років та досвід роботи у сфері захисту інформації, розуміти законодавство та принципи планування захисту у цій сфері. Відповідальний за службу захисту інформації повинен виконувати такі функції:

- розробити політику забезпечення захисту інформації та забезпечити її реалізацію;
- відповідає за роботу служб захисту інформації та забезпечення захисту конфіденційної інформації;
- планує та безпосередньо керує роботою відділу захисту інформації, несе персональну відповідальність за виконання покладених на відділ завдань, забезпечує неухильне виконання підлеглими посадових обов'язків і правил внутрішнього трудового розпорядку;
- особисто бере участь у реалізації найскладніших заходів із забезпечення захисту інформації підприємства;
- розробити план дій на випадок надзвичайної ситуації та проводити регулярне навчання підлеглих;

- керувати службовими розслідуваннями;
- організовує взаємодію відділу захисту інформації з іншими підрозділами;
- Розробити інструкції щодо поводження з комерційною таємницею для осіб, уповноважених працювати з відповідними документами;
- організовувати розробку рекомендацій з удосконалювання функціонування Служби захисту інформації ;
- здійснювати керівництво відділом охорони;
- крім того, виконувати функції юриста: розробка, ведення й оновлення основних документів з метою закріплення в них вимог забезпечення безпеки й захисту конфіденційної інформації [31].

Для забезпечення повноцінного організаційного й правового захисту інформації необхідно розробити пакет документів, а саме:

- положення про конфіденційну інформацію підприємства;
- перелік документів підприємства, що містять конфіденційну інформацію;
- ·інструкцію із захисту конфіденційної інформації в інформаційній системі підприємства;
- пропозиції щодо внесення змін до Статуту підприємства;
- пропозиції щодо внесення змін до трудового договору, контракту із керівником і колективного договору;
- угоду зі співробітником про нерозголошення конфіденційної інформації підприємства;
- зобов'язання співробітника про нерозголошення конфіденційної інформації підприємства після звільнення;
- пропозиції щодо внесення змін до Правил внутрішнього розпорядку підприємства (у частині регламентації засобів фізичного захисту інформації й питань режиму);
- пропозиції щодо внесення змін до посадового (штатного) розкладу підприємства (штату Служби захисту інформації);

- пропозиції щодо внесення доповнень до посадових інструкцій усього персоналу;
- відомість ознайомлення співробітників підприємства з Положенням про конфіденційну інформацію й Інструкцію із захисту конфіденційної інформації в інформаційній системі підприємства;
- план проведення занять із персоналом щодо збереження й нерозголошення конфіденційної інформації;
- пропозиції щодо внесення змін до структури інтерв'ю при прийманні на роботу (уточнення зобов'язань інформаційного характеру з останніх місць роботи);
- пропозиції щодо внесення доповнень до стандартних договорів з контрагентами.

Ці документи відіграють важливу роль у забезпеченні безпеки підприємства.

Створення нового відділу дозволяє контролювати усі процеси захисту інформації, а задачею інших відділів є організувати діяльність так, аби не було витоку інформації та не створювати додаткові проблеми для компанії в загальному.

ІТ-відділ компанії «Макош» відповідає за технічне оснащення (ноутбуки, комп’ютери, телефони, створює електронні пошти, надає паролі та інше), тому важливо налаштувати все так аби не було втручання у технічну систему по сторонніми.

Система захисту інформації, що обробляється з використанням технічних засобів, будується за певними принципами. Це обумовлено необхідністю протидії цілої низки загроз безпеки інформації. Основним принципом протидії загрозам безпеки інформації, є превентивність вжитих заходів захисту, так як усунення наслідків прояви загроз вимагає значних фінансових, часових і матеріальних витрат.

Технічні правила для захисту інформації в компанії включають в себе конкретні технічні заходи та вимоги, які допомагають забезпечити безпеку

даних та інформаційних ресурсів. Ось кілька ключових технічних правил, які можуть служити основою для політики безпеки інформації в компанії:

1. Шифрування даних:

Створити сильні алгоритми шифрування для захисту конфіденційної інформації під час передачі та зберігання даних.

2. Використання безпечних паролів:

Встановити вимоги до складності паролів, включаючи використання великих і малих літер, цифр і спецсимволів.

Заохочувати регулярну зміну паролів.

3. Двофакторна аутентифікація (2FA):

Вимагати використання двофакторної аутентифікації для підвищення рівня безпеки облікових записів.

4. Управління доступом.

Встановити систему управління доступом, яка обмежує права доступу користувачів на основі їхніх ролей та обов'язків.

5. Антивірусні заходи:

Встановити та регулярно оновлювати програмне забезпечення антивірусного захисту на всіх пристроях.

6. Інформаційна безпека мережі:

Захищати безпеку бездротових мереж за допомогою шифрування та інших заходів.

7. Шифрування електронної пошти:

Використовувати шифрування для захисту електронної пошти, особливо якщо вона містить конфіденційну інформацію.

8. Фізична безпека обладнання:

Захищати фізичний доступ до серверних приміщень та інших інформаційних ресурсів.

9. Найняти експертів

Найголовніше і важливіше – правильно вибрати компанію, яка грамотно та відповідально проведе аудит IT-інфраструктури та безпеки та допоможе зі

створенням надійної системи захисту даних. Співробітники IT Ресурс мають величезний досвід у вирішенні таких проблем та готові допомогти представникам малого та середнього бізнесу у створенні інформаційної безпеки компанії. Однією із таких компаній є компанія «Ресурс» яка проводить:

- ✓ Абонентське обслуговування комп'ютерів (професіонали з дипломами про вищу освіту та багаторічним досвідом у IT-сфері. Вони добре знаються на системному адмініструванні, аутсорсингу обслуговування комп'ютерів, проектуванні та прокладанні локальних мереж)
- ✓ Оренда хмарного сервера (це дійсно винахід майбутнього, який дозволяє не завантажувати ваш комп'ютер, користуватися необхідною інформацією з будь-якого пристрою та з будь-якої точки світу, а також отримувати величезні обсяги пам'яті для зберігання та обробки даних)
- ✓ Аудит IT-безпеки (обов'язковий інструмент для кожного офісу у 21 столітті. Грамотний аудит дозволить забезпечити безпеку ваших даних, цінних паперів організації та не поставить під загрозу ваші фінанси та бізнес загалом. Ми пропонуємо найкращий продукт на ринку, який захистить вас від неприємних несподіванок) [32]

Ці технічні правила мають на меті створити повний і високоефективний механізм захисту інформації, який враховує різноманітні аспекти технічної безпеки.

Для HR-відділу потрібно розробити навчання для нових співробітників, що захисту інформації та її конфіденційності. Включити в навчання такі основні аспекти, які допоможуть новому працівнику зрозуміти усю систему захисту та допоможуть уникнути витоку інформації. Наведено основні задачі для створення навчання:

1. Основи безпеки інформації:

Визначення термінів і понять (конфіденційність, цілісність, доступність, аутентифікація, авторизація).

Знайомство з основними загрозами безпеки інформації в цілому.

2. Правила користування системами:

Правила створення, збереження та використання паролів.

Запобігання використанню спільних паролів та записів.

3. Правила користування технічним оснащенням.

Разом із відділом IT підготувати правила користування робочим комп'ютером та телефоном.

4. Безпека електронної пошти:

Визначення та уникання фішингових атак, зауважити про дуже часті випадки та якщо виникла дана ситуація звертатись у відділ IT або Службу захисту інформації .

Використання безпечних вкладень та сайтів.

5. Загальна свідомість про безпеку:

Відомості щодо можливих загроз та як їх виявляти.

Запобігання соціальній інженерії та іншим видам атак.

6. Процедури реагування на інциденти:

Звітність інцидентів безпеки та процедури повідомлення.

Застосування плану відновлення в разі інциденту.

7.Докладно розповісти, що містить в собі комерційна таємниця компанії Макош, які дані не можна розголошувати.

Важливо донести до нового співробітника компанії, що потрібно здійснювати захист інформації починаючи з себе, а також, що деякі необдумані вчинки можуть призвести до серйозних наслідків.

Також відділ HR повинен найняти фахівця з ведення обліку кадрів компаній Макош. Обліковець буде займатись виключно:

- Веденням кадрового обліку та підготовка документації.

- Реєстраціями та веденням персональних картотек співробітників.

- Забезпеченням дотримання законодавства та політик компанії з питань кадрів.

- Участь у процесі звільнення працівників та виведення їх з роботи за усіма правилами законодавства.

- Збиранням, оновлення та управління персональними даними працівників.

- Веденням документації з питань кадрів, включаючи контракти та інші документи.

Це забезпечить компанію чіткими правилами ведення обліку робочих документів, де буде все структуровано, організовано, й підготовлено до передачі в бухгалтерію, що забезпечить постійний захист інформації.

Бухгалтерська інформація є основною складовою економічної та інформаційної безпеки підприємства. Комерційна таємниця у свою чергу забезпечує обмежений доступ до життєво необхідної інформації підприємства. Оскільки вона передбачає захист переважно бухгалтерської інформації і є організаційно-правовим заходом інформаційної безпеки, невід'ємною його складовою, основним елементом захисту комерційної таємниці від впливу негативних факторів слід вважати бухгалтерський облік, який є передумовою порядку та безпеки на підприємстві. Тобто організація бухгалтерського обліку на підприємстві є досить важливим і зваженим заходом, оскільки від нього в подальшому буде залежати ефективне функціонування підприємства та його безпека.[33]

Відділу бухгалтерію у компанії Макош потрібно створити систему передачі інформації в архів на зберігання.

Архівація документів – важливий етап управління документообігом в організації. На рис. 3.4 подано загальна послідовність і рекомендації щодо цього процесу.

1. Підготовка до Архівації:

Розділення документів на групи відповідно до їхнього типу чи теми.

Призначення дати закінчення строку зберігання кожної групи документів.

2. Оформлення Документації:

Заповнення акту передачі документів в архів, який включає інформацію про передані документи, їхню кількість та строк зберігання.

3. Позначення та Сортування:

Позначення кожної групи документів чіткими етикетками.

Сортування їх відповідно до категорій та строку зберігання.

4. Зберігання в Архіві:

Розміщення документів в архівних коробках чи папках з урахуванням збереження порядку та доступності для подальшого пошуку.

5. Створення Журналу:

Заповнення журналу архівації, в якому вказана детальна інформація про кожен документ, його місцезнаходження та строк зберігання.

6. Захист та Контроль:

Забезпечення захисту документів від збитків, вологи, пилу та інших негативних факторів [34].

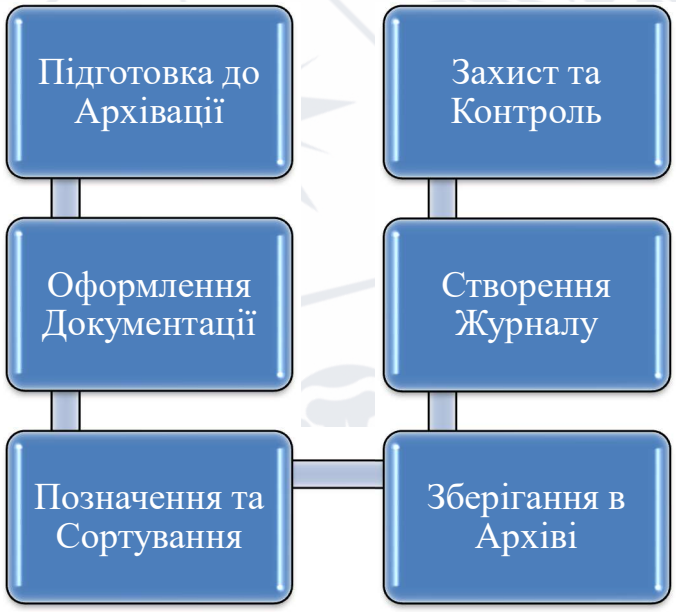

Рисунок 3.4 – Загальна послідовність архівації документів

Здійснення періодичної перевірки стану архіву та відновлення за необхідності.

Процес передачі та архівації документів повинен відповідати внутрішнім політикам компанії та вимогам законодавства.

Ретельне планування та систематичний підхід гарантують ефективність управління документообігом та захищенням інформації.

Запропонований механізм захисту інформації у компанії Макош наведений на рис. 3.5.

МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЇ

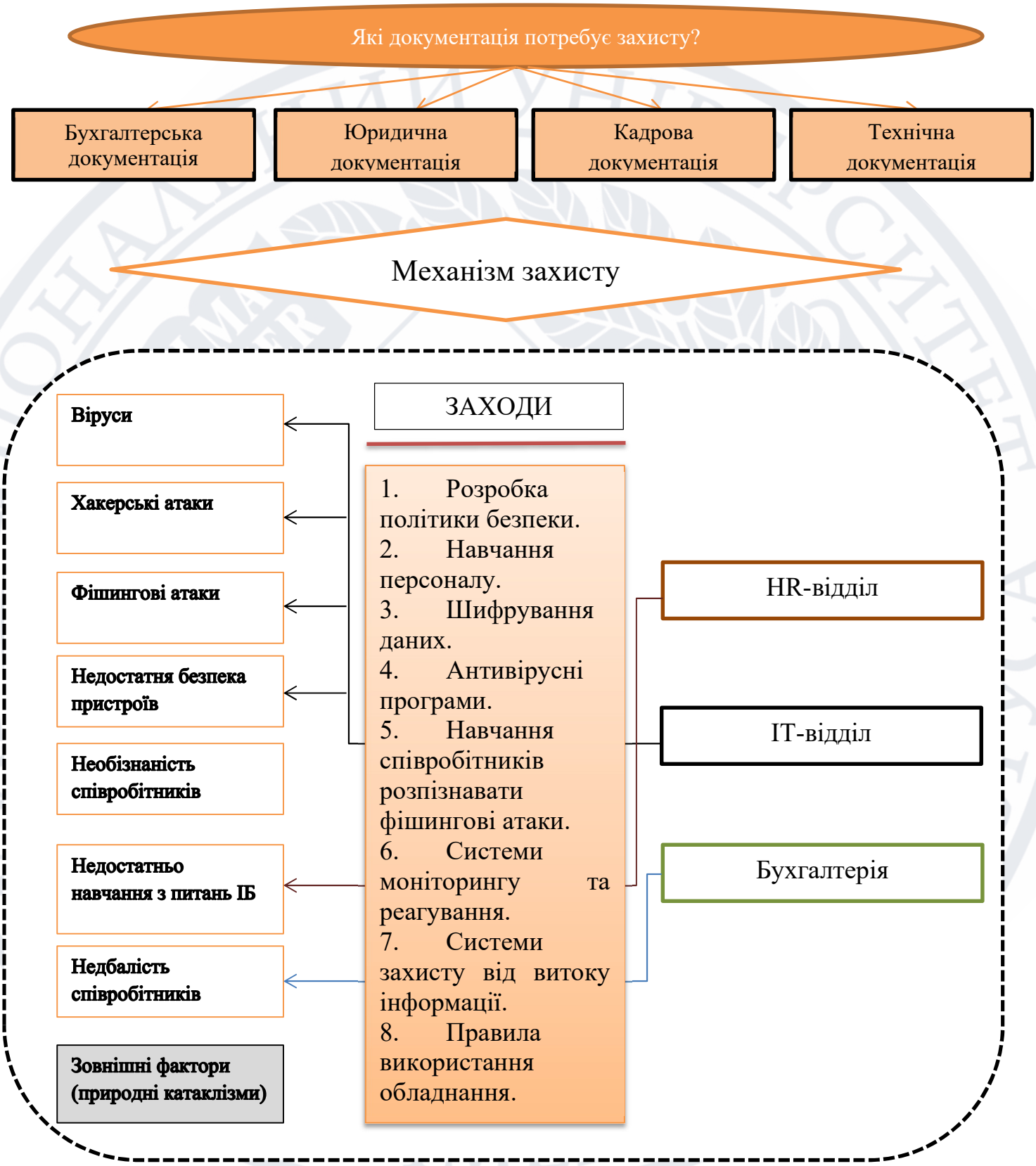

Рисунок 3.5 – Механізм захисту інформації в компанії «Макош»

Отже, механізм захисту інформації у компанії «Макош» повинен виглядати саме таким чином. У механізмі наведено проблематику, а саме відкриті загрози, які можуть бути для інформації, документації у компанії «Макош» (віруси, хакерські атаки, фішингові атаки, недостатня безпека пристроїв, необізнаність співробітників, недостатньо навчання з питань інформаційної безпеки, недбалість співробітників,зовнішні фактори, природні катаклізми). Наведено відділи, які найбільше співпрацюють з технічним забезпеченням – ІТ; робота з документацією, кадровими справами – бухгалтерія; а також з людьми,працівниками, новими співробітниками – HR-відділ. Ці відділи несуть відповідальність за свою закріплену зону відповідальності, а також повинні застосовувати такі заходи для захисту інформації: Розробка політики безпеки.

1. Навчання персоналу.
2. Шифрування даних.
3. Антивірусні програми.
4. Навчання співробітників розпізнавати фішингові атаки.
5. Системи моніторингу та реагування.
6. Системи захисту від витоку інформації.
7. Правила використання обладнання.

Якщо, кожний працівник і відділи будуть відповідально ставитись до конфіденційності даних, дотримуватись механізму захисту інформації, тоді рівень витоку інформації й інших загроз знизиться до мінімального.

На сьогодні забезпечення належного стану інформаційної безпеки вимагає не просто розробки індивідуальних механізмів захисту, а впровадження системного підходу, що включає комплекс взаємопов’язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових заходів), тощо) [35]. Основна мета будь-якої системи інформаційної безпеки - створити умови для функціонування підприємства, запобігти загрозі його безпеці, захистити законні інтереси підприємства від незаконних посягань, запобігти незаконному привласненню,

витоку, втраті, витоку фінансових ресурсів. , і підроблено. І знищити офіційну інформацію, щоб забезпечити виробничу діяльність усіх відділів підприємства в рамках.

Висновки до розділу 3

У розділі 3 магістерської роботи автором розглянуто методи удосконалення системи захисту інформації, а також розроблено механізм захисту інформації у компанії «Макош» згідно з проблематикою досліджуваною раніше

Визначено, що основне завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Тобто, засоби захисту документації мають застосовуватися одночасно і під керівництвом.

Історія інформаційної безпеки показує, що стовідсоткового захисту від зловмисників не існує. Кіберзлочинці активно і з великим успіхом розробляють технології подолання існуючих систем захисту і проникнення в мережу. Опинившись ж всередині мережі, вони приступають до злому внутрішніх ресурсів підприємства та пошуку цінної інформації. Саме для цього необхідним є впровадження процесу управління ризиками інформаційної безпеки. Щоб успішно протидіяти сучасним кіберзлочинцям, необхідно розробити механізм захисту інформації.

Інформаційна безпека підприємства відіграє дуже важливо роль у розвитку компанії, тому дуже важливо не уникати, а навпаки сконцентрувати свою увагу на захисті інформації, це важливо для уникнення майбутніх дуже серйозних проблемю. Інформаційна безпека підприємства відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві.

Збереження нормального робочого процесу компанії залежить від безпеки її інформації, технологій і бізнес-процесів. Недостатній захист може призвести до перебоїв у роботі та втрати продуктивності.

Запропоновано механізм захисту інформації та документації для компанії «Макош», а також запропоновано найняти спеціально навчених людей, які проведуть загальний аналіз, запропонують свої новітні й сучасні технології для забезпечення повного захисту інформації.

Розглянути створення нового відділу, який буде контролювати, а також забезпечувати усі етапи механізму захисту інформації. Виявляти й максимально перекривати потенційно можливих каналів доступу до інформації, а також вчасне виявлення.

ВИСНОВКИ

У ході проведеного дослідження у рамках виконання магістерської кваліфікаційної роботи автором було визначено теоретичні основи інформації, захисту інформації, основні завдання, етапи. Так, сутність організації захисту інформації відіграє дуже важливу роль в розвитку компанії. Тому, можна зробити висновок, що механізм захисту інформації є фундаментом для успішної діяльності.

Розглянуто особливості організації системи захисту інформації на підприємстві, де визначено , що правильна організація захисту інформації здатна впливати на покращення оперативності, економності, надійності функціонування апарату управління та організації культури праці працівників. Виявлено чіткий взаємозв'язок організації системи захисту інформації з ефективною діяльністю підприємства.

При правильно налаштованій системі організації захисту інформації на підприємстві зменшуються витоки інформації з бази даних клієнтів, інформація про бізнес процеси та інші важливі фактори в діяльності підприємств.

Визначено основні джерела загроз системи захисту інформації:

- проблеми, які можуть виникати з комп'ютерним обладнанням чи софтом;
- несправність поведінки операційних процесів;
- явні чи приховані недоліки інтерфейсів/протоколів;
- характеристики систем, що є частиною великої системи;
- важкі умови експлуатації ПЗ та комп'ютерної техніки;
- недбалість персоналу/користувачів.

Проведено аналіз ефективності системи захисту інформації на підприємствах. Метою аналізу інформаційної безпеки є виявлення вузький місць організації захисту документації на підприємстві та загрози які можуть

нанестись безпеці. Процес, покликаний дослідити та оцінити рівень захисту інформаційних систем організації.

Виокремлено проблематику організації захисту інформації у компанії «Макош». За допомогою усного інтерв'ю з керівниками відділів досліджено, що у компанії дуже низький рівень організації захисту інформації, де немає конкретно механізму і плану для уникнення й передбачення ураження інформаційної безпеки. Також, необізнаність працівників про конфіденційність, неорганізовано належним чином технічні засоби для співробітників, а також повне відсутнє навчання новий працівників для обізнаності базових навичок для захисту інформації компанії.

Виявлено методи удосконалення системи захисту інформації у компанії «Макош», які передбачають собою створення нового відділу, а саме Служби захисту інформації, яка буде контролювати, організовувати усі рівні механізму захисту інформації. Також, забезпечення захисту інформації підприємства необхідне систематичне виконання етапів, які попередять витік інформації.

З метою вирішення даних проблемних питань було розроблено рекомендації для створення механізму захисту інформаційних систем, документацій.

Розроблено чіткий механізм захисту інформації та документації у компанії «Макош», де кожний відділ, який найбільше співпрацює з інформаційними технологіями, з документацію, а також з співробітниками, матиме конкретні задачі, для забезпечення захисту. Основною рекомендацією є найняти організацію, яка проведе структурований аналіз в середині компанії, який допоможе знайти проблеми, а також їх вирішення й це не несе значних затрат, адже така організація працює одноразово.

Дані рекомендації дають змогу вирішити усі проблемні питання існуючої системи та відкриває перспективи для її подальшого покращення та розвитку у розрізі саме покращеного механізму захисту інформації

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Поняття інформація. URL: https://dl.nure.ua/pluginfile.php/468/mod_resource/content/3/content/content2.html

2. Барасюк Я. М., Стець О. В. Інформаційні системи і технології в економіці: навч-метод. посіб. Чернівці: ЧТЕІ КНТЕУ. 2016. 409 с.

3. Інформація та інформаційні системи. URL: https://elearning.sumdu.edu.ua/free_content/lectured:c5dfdb13db13a6099b7e1489d805156fd10127f0/20200921190435//1782630/index.html

4. Власник інформації має право на власний розсуд віднести зазначену інформацію до конфіденційної або комерційної таємниці. URL: https://svp.tax.gov.ua/media-ark/news-ark/558389.html

5. Технічний захист інформації. URL: https://tzi.com.ua/main1ua.html

6. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки: навч. пос. Вінниця: ВНТУ 2018. 317 с.

7. Антонюк А. О. Основи захисту інформації в автоматизованих системах: навч. посіб. Київ: КМ Академія, 2003. 244 с.

8. Верховна Рада України. (2007, січ. 9). Закон № 537-V, Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. URL:: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text (Дата звернення: 15.05.2022).

9. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту у інформації : навч. посібник. Х. : Вид. ХНЕУ, 2013. 476 с.

10. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

11. Система захисту цінної інформації і конфіденційних документів. URL: https://buklib.net/books/33445/

12. Словник законодавчих термінів. Зберігання інформації. URL: https://web.archive.org/web/20150622115127/http://zakon.nau.ua/doc/?uid=1078.4723.0

13. Кримінальний кодекс України Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю. URL: https://kodeksy.com.ua/kriminal_nij_kodeks_ukraini/statja-231.htm

14. Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів. URL: https://zakon.rada.gov.ua/laws/show/z0571-12#Text

15. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. URL: https://www.kmu.gov.ua/npas/32791826

16. Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів. URL: https://zakon.rada.gov.ua/laws/show/z0571-12#Text

17. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання : Наказ Міністерства юстиції України від 11.11.2014 р. № 1886. База даних «Законодавство України». URL: https://zakon2.rada.gov.ua/laws/show/z1421-14 (дата звернення: 24.03.2019)

18. Головльов С. Захист інформації на підприємстві – забезпечення безпеки даних та подолання ризиків. URL: https://resit.com.ua/zachist-informacii-na-pidpriemstvi/

19. Гапак О. М., Глебена М. І. Захист інформації в комп'ютерних системах: підручник. Ужгород : ПП "АУТДОР-ШАРК, 2021. 184 с.

20. Що таке інформаційна безпека компанії? URL: https://resit.com.ua/sho-take-informazijna-bezpeka-kompanii/

21. Основи управління інформаційною безпекою. URL: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf

22. Сайт компанії «Макош». URL: https://makosh-group.com.ua/

23. Механіки соціальної інженерії та як від них уберегтися. URL: https://finance.ua/ua/goodtoknow/socialna-inzheneria

24. Гончаренко Є. О. Вибір підходу до оцінки ризиків інформаційної безпеки для підприємств роздрібної торгівлі. Дипломна робота; науковий керівник Коломицев М.В. Київ, 2019, 92 с.

25. Кримінальний кодекс України Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю. URL: https://kodeksy.com.ua/kriminal_nij_kodeks_ukraini/statja-231.htm

26. Стаття 232. Розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках. URL: https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_232/

27. Відповідальність за ведення підприємницької діяльності без державної реєстрації. URL:https://kyivobl.tax.gov.ua/media-ark/news-ark/print-424520.html

28. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства *Управління проектами та розвиток виробництва*. 2014. № 4. С. 28-39. URL: http://nbuv.gov.ua/UJRN/Uprv_2014_4_6.

29. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації: навчальний посібник. Одеса. 2015. 264 с.

30. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту у інформації : навчальний посібник. Х.: Вид. ХНЕУ, 2013. 476 с.

31. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем: підручник. Київ: Видавнича група BHV, 2009. 608 с.

32. Сайт компанії Ресурс. URL: https://resit.com.ua/about-us/

33. Мелень О. В. Організація бухгалтерського обліку : конспект лекцій для студ. спец. «Облік і аудит» всіх форм навч.. Харків, 2015. 84 с.

34. Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text

35. Носок С. О., Фаль О. М., Ткач В. М. Управління інформаційною безпекою: конспект лекцій: навч. посіб. для студ. спец. 125 «Кібербезпека» КПІ ім. Ігоря Сікорського; Київ, 2021. 258 с.

36. Аналіз інформаційної безпеки: особливості та переваги нової послуги від Softline. URL: https://softline.org.ua/news/analiz-informacijnoi-bezpeki-osoblivosti-ta-perevagi-novoi-poslugi-vid-softline.html

37. Некраш І. І. «Дослідження проблем оцінки відповідності функціональних компонентів систем захисту інформації»: магістерська робота, науковий керівник Горицький В. М. Київ, 2018. 93 с.

38. Механізм захисту комерційної таємниці підприємства. URL: http://megalib.com.ua/content/2777_2_Mehanizm_zahisty_komerciinoi_taemnici_pidpriemstva.html

39. Горник В.Г., Кравченко С.О. Механізми забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Державне управління. 2020. Т. 31(70). № 2. С. 206-212. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2020/2_2020/36.pdf

40. Корженівський О. Загальне поняття інформації. Пульсар. Київ, 2001. № 4. С. 7.

41. Субіна Т. Поняття і сутність інформації у просторі держави. *Науковий вісник Національної академії ДПС України*. 2004. № 4 (26). С. 20–21.

42. Антонюк А. О. Основи захисту інформації в автоматизованих системах. Київ. 2006. 244 с.

43. Закон України від 1992.10.02 № 2657-XII "Про інформацію" URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

44. Захист інформації на підприємстві – забезпечення безпеки даних та подолання ризиків. URL: https://resit.com.ua/zachist-informacii-na-pidpriemstvi/

45. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. Київ. 2004. 508 с.

46. Лисак Н. В., Міронова Ю. В., Рудковська О. Л. Методичний підхід до оцінювання захисту інформації на підприємствах. *Наукові праці ВНТУ*, 2015, № 3. С. 1-10.

ДОДАТКИ

ДОДАТОК А

ПОПЕРЕДЖЕННЯ ІТ-ВІДДІЛОМ У ЗАГАЛЬНУ ГРУПУ ПРО НОВУ СХЕМУ ШАХРАЙСТВА