МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ЦЕНТР ПІСЛЯДИПЛОМНОЇ ОСВІТИ, ДИСТАНЦІЙНОГО ТА ЗАОЧНОГО НАВЧАННЯ

Кафедра менеджменту

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІЗАЦІЇ В СУЧАСНИХ УМОВАХ

здобувача вищої освіти
освітнього ступеня «бакалавр»
4 курсу заочної форми навчання
спеціальності 073 «Менеджмент»
Віктор КУШНІР

Науковий керівник
к.е.н., доц. Наталія БЛАГА

Рецензент:
к.е.н., доцент Ірина ПРИЙМАК

Кваліфікаційна робота допущена до захисту
«___» _____ 2023 р., протокол № ____

Завідувач кафедри менеджменту
_____Галина ЛЕСЬКІВ

Львів
2023

АНОТАЦІЯ

Кушнір В. Інформаційна безпека організації в сучасних умовах. Рукопис.

Дослідження на здобуття освітнього ступеня «бакалавр» за спеціальністю 073 «Менеджмент», Львів, 2023.

У першому розділі проведено теоретичне дослідження основних аспектів інформаційної безпеки організації. У другому розділі проведено аналіз системи інформаційної безпеки ТОВ «Глобал Вест» та виокремлено сучасні підходи до розробки інформаційної безпеки ТОВ «Глобал Вест».

На основі опрацювання матеріалів теоретичного та практичного характеру зроблені відповідні висновки та обґрунтовано конкретні пропозиції.

Ключові слова: інформація, безпека, інформаційна безпека, управління, підприємство.

ABSTRACT

Kushnir V. Information security of the organization in modern conditions. Manuscript.

Research for obtaining a bachelor's degree in the specialty 073 "Management", Lviv, 2023.

In the first chapter, a theoretical study of the main aspects of the organization's information security is carried out. In the second chapter, an analysis of the information security system of Global West LLC is carried out and modern approaches to the development of information security of Global West LLC are highlighted.

Based on the processing of materials of a theoretical and practical nature, appropriate conclusions were drawn and concrete proposals were substantiated.

Keywords: information, security, information security, management, enterprise.

Зміст

ВСТУП

У сучасному глобальному світі інформація має ознаки головної цінності й уміння оперувати достовірною, повною та актуальною інформацією дає суттєві переваги у конкурентній ринковій боротьбі. Вона є ключовим елементом для успішного функціонування не лише підприємств, а й цілих держав та окремих громадян, адже її можна використати для прийняття рішень, розвитку бізнесу, забезпечення національної безпеки та інших цілей. Однак, наявність великої кількості інформації також створює проблеми та ризики: проблеми того, що оперувати значними обсягами інформації з належною оперативністю практично не можливо без сучасного розвинутого інструментарію, а ризики пов'язані із небезпеками, як от крадіжки інформації, шпигунство, шахрайства, вірусні атаки та інші загрози. Тому захист інформації та її безпека є важливими завданнями в усіх сферах діяльності.

При вивченні інформації та різних її аспектів, у тому числі безпекового, успішно поєднують теоретичні та емпіричні підходи. Теоретичні дослідження та моделі учених із світовим ім'ям дали змогу розвинути підходи до оцінки кількості інформації, способів її кодування, методів аналізу та шифрування, лягли в основу розуміння фундаментальних закономірностей поводження з інформацією у різних видах та формах; потреби практики ж знайшли способи побудови електронних машин, котрі значно розширили можливості по роботі із даними, розробили і запровадили різні формати даних та алгоритми їх обробки. Без глибокого розуміння принципів поводження із інформацією існують ризики втрати цінної інформації, її викрадення зловмисниками і навіть формулювання невірних висновків при прийнятті рішень. Вміння працювати із інформацією у сьогоднішньому світі дедалі більше стає основним вмінням спеціаліста. При цьому розкриваються різні аспекти роботи з інформацією: технічний, семантичний, ціннісний та інші.

Кожне підприємство у своїй роботі використовує інформацію. Абсолютна більшість підприємств використовує сучасні інформаційні технології та автоматизовані інформаційні системи. Для багатьох, а можливо й більшості підпри-

ємств сьогодні інформаційні технології становлять суттєву частину сфери діяльності підприємства у формі взаємодії з клієнтами, рекламних заходів, інструментів управління тощо. У значної частки найбільш високоприбуткових підприємств інформаційна складова є основним продуктом діяльності: консультаційні послуги, інформаційна підтримка, інші види діяльності. Тому вразливість підприємств до інформаційних атак може бути різною, проте вона ніколи не є нульовою. А отже інформаційна безпека підприємства є важливим аспектом його функціонування і дослідження інформаційної безпеки підприємства чи організації **є актуальною темою** для досліджень.

Дослідження питання формування іміджу підприємства та його значення для успішної діяльності організації стали предметом дослідження багатьох зарубіжних та вітчизняних вчених, а саме: А. Авраменко, І. Адамська, В. Грищенко та ряд інших дослідників.

Метою дослідження є дослідження інформаційної безпеки та її прояви у діяльності підприємства чи організації, а також інформаційна оцінка та обґрунтування основних підходів до підвищення рівня розвитку інформаційної безпеки ТОВ «Глобал Вест».

Для досягнення поставленої мети треба вирішити наступні завдання;

- Вивчити визначення інформації та прийоми і методи роботи із нею;
- Дослідити місце інформаційної безпеки у системі безпеки організації;
- З’ясувати фактори інформаційної безпеки ТОВ «Глобал Вест»;
- Дослідити механізми управління інформаційною безпекою підприємства;
- Розглянути перспективи підвищення рівня інформаціної безпеки ТОВ «Глобал Вест».

Об’єктом дослідження є інформаційна безпека ТОВ «Глобал Вест».

Предметом дослідження є теоретико-методологічні основи та практичні рекомендації щодо покращення інформаційної безпеки підприємства.

Методи дослідження. Для досягнення поставленої мети в роботі використано такі загальні наукові та спеціальні методи як систематизації та

узагальнення теоретичних досліджень, емпіричних оцінок, порівняльного аналізу та логічного узагальнення результатів.

Інформаційною базою дослідження є Закони України, підручники, навчальні посібники, статті, автореферати, монографії та інші наукові праці вітчизняних і зарубіжних вчених.

Апробація результатів дослідження. Основні положення та результати дослідження кваліфікаційної роботи розглядалися на проведенні круглого столу за темою «Безпекові аспекти управління організаціями в умовах війни та повоєнної відбудови держави».

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ВИВЧЕННЯ ІНФОРМАЦІЇ ТА ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Поняття, форми та методи роботи із інформацією

Поняття "інформація" доволі широке. Згідно словника іншомовних слів млово "інформація" походить від латинського "informatio", що означає "роз'яснення", і може означати або повідомлення про щось, або ж відомості про події, факти, процеси тощо, що їх сприймають люди, інші живі організми, керуючі машини або інші системи. Важливим нюансом цього визначення є те, що інформація не існує як окремий матеріальний об'єкт чи феномен речового світу, а виражається при передачі від одного суб'єкта до іншого.

Класичні визначення інформації використовують синонімічні терміни: дані, відомості, повідомлення тощо. Можна зустріти визначення: "Інформація – це знання або факти, які передаються, зберігаються та оброблюються в певний спосіб для подальшого використання". У роботі [13] згадується два визначення, більш загальне:

Інформація – це відомості, що є об'єктом зберігання, передавання та перетворення;

та більш вузьке, пов'язане із поняттями дані та повідомлення: отже, дані – це відомості, подані у формалізованому вигляді (висловлені словами, записані формулами чи на магнітну стрічку, зображені графічно тощо). Якщо ці дані мають бути передані від джерела до респондента, вони мають бути оформлені у вигляді повідомлень (фактично, повідомлення повинно бути зрозумілим респонденту, інакше воно не донесе адресату потрібної інформації; фактично джерело і адресат повинні мати спільний канал комунікації, інакше кажучи, знайти спільну мову). Під час використання, передачі повідомлень, вони несуть інформацію, причому лише у випадку, якщо ці повідомлення відзначаються новизною, формально – знижують невизначеність ситуації. Тому тлумачення терміну "інфор-

мація" можливе на різних рівнях узагальнення: від комп'ютерного "це задана кількість біт" до загально-філософського "це відображення дійсності".

Інформація може мати різні рівні значимості та корисності в залежності від того, що саме вона містить і як вона може бути використана. Наприклад, інформація про стан здоров'я людини може бути важливою для лікаря, але не мати великої цінності для іншої людини, інформація про напруження у елементі конструкції багато що скаже інженеру-механіку, проте мало придастся комусь іншому, нотний запис зможе прочитати особа із музичною освітою, проте це буде лише картинка для кого, хто нот читати не вміє.

Загалом існують різні аспекти вивчення інформації, найбільш поширені: технічний, семантичний та прагматичний аспект. Найбільш об'єктивним і повно дослідженим є технічний аспект, який охоплює різноманітні технології та методи, які допомагають збирати, зберігати, обробляти та передавати інформацію. До таких технологій відносять:

- комп'ютерні технології (застосування ЕОМ як апаратного забезпечення та відповідного програмного забезпечення, як от бази даних, електронні таблиці, текстові редактори, облікові системи та інші, дозволяють збирати та обробляти великі обсяги інформації);
- інтернет-технології (можливість доступу до глобальної мережі та технології обміну даними у мережа, обмін інформацією з іншими користувачами; ефективність значно зростає при розробці технологій роботи із великими масивами даних (big data)).
- комунікаційні технології (телефонія, електронна пошта, месенджери та соціальні мережі, дозволяють швидко та ефективно передавати інформацію від одного користувача до іншого, до групи користувачів (розсилки, канали), чи від різних користувачів до одного центру (інтернет-голосування, конференції), а також забезпечувати надійність та безпеку таких обмінів даними.
- технології штучного інтелекту (аналіз даних, системи й алгоритми машинного навчання, методи аналізу даних й розпізнавання образів, у

перспективі системи прийняття рішень на основі виявлених складних зв’язків між даними).

- технології захисту інформації (технології, що дозволяють захистити інформацію від несанкціонованого доступу, крадіжки та розголошення; також важливими, хоч менш обговорюваними є технології захисту даних від випадкових втрат – дублювання, бекапи, зберігання даних у хмарі тощо. До технологій захисту від доступу відносяться шифрування даних, захисні мережеві екрани, паролі, аутентифікація користувачів та інші).

Ці технології тісно пов’язані між собою, наприклад від способу передачі даних може залежати потреба у його захисту на апаратному чи програмному рівні. Таким чином, вивчення інформації з технічної точки зору охоплює різноманітні аспекти зберігання, передачі, обробки та захисту.

Семантичний (від грецького σημα – знак, ознака, смислова одиниця) аспект вивчення інформації стосується того, як сама інформація трактується та розуміється людиною. Основна ідея семантичного аспекту полягає у тому, що інформація сама по собі не має значення, важливо лише те, як її розуміють та використовують люди. Саме тому при передачі інформації від джерела до адресата вони понинні використовувати спільну мову, без різниці, чи це природна мова, чи мова жестів, а чи мова дорожних знаків.

Приклади питань, відповідь на які дає семантичний аспект інформації: як інформація розуміється людиною (наприклад, термін "шар" може мати різні значення для різних людей)? Які зв’язки існують між різними елементами інформації (наприклад, зміст речення може змінюватись докорінно у залежності від порядку слів, розділових знаків чи інтонації)? Як інформація впливає на сприйняття та поведінку людей (різні люди дуже по різному реагують на одне і те ж повідомлення: анекдот може бути смішним для одних осіб і ілком не смішний для інших; інший приклад – рекламна інформація може впливати на поведінку покупців, а як саме – дуже хотіди б знати маркетологи і спеціалісти із ПР). Як інформація пов'язана з культурними та соціальними контекстами? Таким чином, семантичний аспект вивчення інформації допомагає розуміти те, як люди

розуміють та використовують інформацію в різних контекстах, що є важливим для ефективного спілкування та взаєморозуміння.

Особливий інтерес становить прагматичний аспект вивчення інформації. Прагматичний аспект вивчення інформації стосується того, як інформація використовується та чим вона корисна для певного суб'єкта у визначений момент часу. Переважно це залежить від того, як вона впливає на поведінку та діяльність людей. Основна ідея прагматичного аспекту полягає у тому, що інформація має бути корисною у реальному житті. Гарним прикладом прагматичного відношення до інформації є літературний персонаж Шерлок Голмс, якого не цікавили відомості щодо астрономічних чи абстрактних фактів, а лише такі, які він міг використати у своїй основній діяльності.

Прагматичний аспект вивчення інформації охоплює такі питання, як:

1. Як можна використовувати інформацію для досягнення певних цілей? Наприклад, як підприємство може використовувати інформацію про своїх конкурентів для розробки ефективної стратегії.

2. Як інформація впливає на прийняття рішень? Наприклад, як інформація про ризики може впливати на рішення про інвестування коштів.

3. Як можна зберігати та організовувати інформацію, щоб вона була корисною та доступною? Наприклад, як користуватися базою даних для зберігання та організації інформації про клієнтів.

4. Як інформація пов'язана з результатами діяльності та прибутком підприємства? Наприклад, як аналіз інформації може допомогти виявити проблемні сфери та підвищити ефективність діяльності підприємства.

Таким чином, прагматичний аспект вивчення інформації допомагає зрозуміти, як інформацію можна використовувати для досягнення конкретних цілей та підвищення ефективності діяльності. Цей аспект є дуже важливим для підприємств та організацій, які потребують ефективного використання усієї доступної інформації.

У комп'ютерних науках інформацію можна подавати в різних форматах та за допомогою різноманітних інструментів. У залежності від форми подання

різняться прийоми та методи роботи з інформацією. Основні форми подання інформації у комп’ютерних науках такі:

- Текстовий формат – це давня і ймовірно найбільш поширена на ЕОМ форма подання інформації, яку можна створювати за допомогою текстових редакторів, таких як Microsoft Word, Word Perfect або Google Docs. Текстовий формат зручний для подання довгих текстів, які можна розбити на розділи та підрозділи з різними заголовками. Традиційно звичайний текст розбивають на речення і абзаци. Розрізняють простий текст (один символ – один або декілька байт) та текст із форматуванням (т.зв. rich text format)
- Графічний формат – це формат, що використовується для створення зображень (у тому числі для зберігання фотографій), діаграм, графіків та інших графічних елементів. Для створення графічних зображень використовуються спеціальні програми для графічного дизайну, такі як Adobe Photoshop чи GIMP. Основні типи графіки – растрова та векторна графіка, поширені формати: jpg, png, tiff, svg, ai та інші.
- Аудіо формат – це група форматів, що використовується для запису звуку та музики. Для створення та редагування аудіофайлів використовуються спеціальні програми, такі як Adobe Audition чи Audacity. Традиційно використовувати запис потокового аудіо (mp3 із різними кодеками) та нотний запис (mid), останній більш економний, хоча менш універсальний, і на сьогодні використовується порівняно нечасто.
- Відео формат – використовується для запису відео та фільмів, зазвичай mp4 та велике розмаїття способів організації запису. Для створення та редагування відеофайлів використовуються спеціальні програми, такі як Adobe Premiere Pro чи Final Cut Pro.
- Програмний код – це формат, що використовується для створення програм та скриптів, фактично це формат інструкцій для комп’ютера, як вирішувати певні задачі. Програмний код можна писати у різних мовах програмування, таких як Java, Python, C++, JavaScript та інші. Вихідний код зазвичай є звичайним текстовим файлом, проте його "слова" є командами,

що мають зміст лише у певній мові програмування (або споріднених мовах) за умови, що програма складена вірно.

- Електронні таблиці – це формат, що використовується для створення табличних даних та їх обробки. Для створення та редагування електронних таблиць використовуються програми, такі як Microsoft Excel або Google Sheets. Сьогоднішні середовища електронних таблиць підтримують вбудовані графічні ілюстрації (діаграми), формули та підпрограми (макроси).

Існують також численні спеціалізовані формати, наприклад для збереження презентацій, статистичних даних, числових та інших. Ці формати можна комбінувати, наприклад, багато сучасних форматів графіки поєднують растрову та векторну графіки, а текстові формати на кшталт MSWord можуть містити формули, таблиці, рисунки, гіперпосилання і навіть відео.

На жаль, не існує одиниці захищеності інформації. Захищеність інформації – це складна і багатовимірна концепція, яка охоплює безліч факторів, таких як конфіденційність, цілісність, наявність, доступність і аутентичність. Кожен з цих факторів може мати свої власні метрики і механізми вимірювання, що залежать від контексту та типу інформації [27]. Тому захищеність інформації оцінюється в комплексі, з урахуванням всіх цих факторів і їх взаємозв'язку.

1.2 Сучасні автоматизовані інформаційні системи та їх місце у діяльності організації

Нині у світі, де швидкість точність та ефективність є ключовими факторами успіху, автоматизовані інформаційні системи є невід’ємною частиною діяльності багатьох організацій. Вони впливають на різні аспекти бізнесу, починаючи від оптимізації робочих процесів до підвищення продуктивності та покращення якості обслуговування клієнтів.

Одним із головних призначень автоматизованих інформаційних систем є автоматизація бізнес-процесів. Це означає, що повсякденні операції, такі як

обробка замовлень, управління запасами, фінансовий облік та інші , виконується автоматично з використанням комп'ютерних програм та спеціальних систем. Це дозволяє організаціям зберігати час і ресурси, а також уникати помилок, котрій пов'язані з людським фактором.

Сучасні автоматизовані інформаційні системи (АІС) забезпечують ефективність та точність обліку та аналізу даних, зменшують час на виконання рутинних задач та покращують якість прийняття рішень.

Використання організацією автоматизованих інформаційних систем може дати перевагу перед конкурентами. Адже швидка обробка даних, автоматизовані бізнес-процеси та зручний доступ до інформації дозволяють підприємством бути більше гнучкими, інноваційними та адаптованими до змін.

Автоматизовані інформаційні системи можуть бути різного типу, включаючи системи управління взаємодією з клієнтами, системи управління виробництвом та постачанням, системи управління проектами, системи управління ресурсами підприємства та інші.

Проте, зберігання, передача та обробка великої кількості даних в АІС можуть створювати ризики для інформаційної безпеки організації [32]. Зокрема, можуть виникати загрози злому систем, витоку даних, шахрайства та інших видів кіберзлочинності.

Отже, забезпечення безпеки АІС та даних, що в них зберігаються, є критично важливим для забезпечення успіху діяльності організації. Це вимагає розробки та впровадження ефективних заходів з інформаційної безпеки, включаючи забезпечення криптографічного захисту, автентифікацію та авторизацію, моніторинг та аудит доступу, резервне копіювання та відновлення даних та інші. Ці інструменти відносять до та реалізують за допомогою програмних засобів АІС. Розрізняють також апаратні засоби АІС. Їх якість, особливо, якщо це стосується каналів зв'язку, також суттєво позначається на інформаційній безпеці підприємства. Розглянемо детальніше на прикладах.

Технічні складові інформаційних систем (ІС) – це апаратні та програмні компоненти, що забезпечують роботу системи. Апаратні складові включають

комп’ютери, сервери, сховища даних, мережеве обладнання та інші пристрої, що забезпечують функціонування ІС. Програмні складові включають операційні системи, бази даних, програмне забезпечення для збору, зберігання та обробки даних, а також інші програми, що забезпечують функціонування ІС.

Технічні складові ІС відіграють важливу роль у забезпеченні безпеки даних інформаційної системи. До завдань технічних складових належить забезпечення захисту інформації від несанкціонованого доступу, захист від вірусів та інших шкідливих програм, а також забезпечення доступу до інформації тільки для користувачів з необхідними дозволами. Отже, технічні складові ІС є ключовими елементами в забезпеченні безпеки інформаційної системи.

Апаратні компоненти (hardware) є одним з важливих елементів інформаційних систем, що забезпечують захист інформації та інформаційну безпеку. Деякі з найбільш важливих апаратних компонентів для забезпечення інформаційної безпеки включають:

Сервери: Сервери є важливим елементом інфраструктури даних та забезпечують збереження, обробку та розподіл інформації. Сервери можуть мати вбудовані механізми захисту даних, такі як файрволи, антивірусні програми та інші.

Роутери та комутатори: Роутери та комутатори забезпечують мережеве з'єднання між пристроями та мережевими ресурсами. Вони можуть мати вбудовані механізми захисту, такі як системи виявлення вторгнень та фільтрації трафіку.

Криптографічні пристрої: Криптографічні пристрої використовуються для шифрування та розшифрування даних. Вони можуть мати апаратне забезпечення для розрахунку криптографічних алгоритмів, що забезпечують високу швидкість та безпеку.

Фізичні пристрої захисту: До фізичних пристроїв захисту відносяться системи контролю доступу, відеокамери та системи виявлення інтрузій. Вони допомагають забезпечити фізичну безпеку приміщень та обладнання.

Бекап-системи: Бекап-системи забезпечують збереження даних в разі випадкового або навмисного їх видалення чи пошкодження. Вони можуть мати вбудовані механізми захисту, такі як шифрування та віддалене збереження.

Наприклад, біометрична аутентифікація на рівні апаратного забезпечення може забезпечити вищий рівень захисту, ніж звичайний пароль. Такі пристрої як сканер відбитків пальців, сканер обличчя та сканер сітківки ока можуть використовуватися для визначення особистості користувача та обмеження доступу до конфіденційної інформації.

Іншим прикладом можуть бути апаратні захисні засоби, такі як апаратні модулі безпеки (TPM – Trusted Platform Module). TPM – це чіп, вбудований в материнську плату комп'ютера або в інші пристрої, який забезпечує функції шифрування, генерації ключів і аутентифікації. Використання TPM може допомогти запобігти атакам на даних шляхом зберігання ключів шифрування та інших конфіденційних даних в захищеному апаратному середовищі.

Крім того, апаратне забезпечення може включати і вбудовані захисні функції, такі як виявлення вторгнень (IDS) і системи попередження про вторгнення (IPS). Ці функції дозволяють системі автоматично виявляти та блокувати спроби несанкціонованого доступу до інформації.

Усі ці апаратні компоненти допомагають забезпечувати безпеку інформації шляхом забезпечення конфіденційності, цілісності та доступності. Крім того, вони можуть допомогти підприємствам виконувати різні регуляторні вимоги з охорони даних і захисту персональної інформації.

Програмні засоби інформаційної безпеки - це програми, призначені для захисту інформації, що зберігається на комп'ютерах, серверах, в мережах інтернет та інших інформаційних системах. Основна мета програмних засобів інформаційної безпеки полягає в запобіганні несанкціонованому доступу до конфіденційної інформації, виявленні інцидентів безпеки, захисті від вірусів та інших шкідливих програм.

Серед програмних засобів інформаційної безпеки можна виділити наступні: антивірусні програми; фаєрволи (мережеві екрани); антишпигунські

програми; криптографічні програми; системи контролю доступу; системи резервного копіювання; системи моніторингу та аудиту.

1.3 Інформаційна безпека організації: види та особливості

Інформаційна безпека є важливим аспектом діяльності будь-якої організації сучасному цифровому світі. Вона відноситься до заходів, що спрямовані на захист інформації від несанкціонованого доступу, використання, руйнування або розголошення. Інформаційна безпека має різні види та особливості, які важливо враховувати при розробці та провадженні заходів щодо захисту організаційний інформації.

Інформаційна безпека підприємства чи організації залежить від багатьох факторів, серед яких можна виділити наступні:

- Люди: найбільшу загрозу для інформаційної безпеки підприємства становлять люди, які взаємодіють з інформаційною системою. Це можуть бути співробітники, клієнти, постачальники, зловмисники та інші. Фактори цієї групи можна поділити на внутрішні і зовнішні, останній можна теж поділити на групи з знаком "плюс" – клієнти, партнери, постачальники тощо, та "мінус" – конкуренти, зловмисники, хакети і т.ін. Саме для людей призначена інформація і саме на її основі приймаються певні рішення, що впливають на стан підприємства.
- Технології: використання застарілих, неактуальних або технологій, котрі потребують оновлення, може призвести до порушень інформаційної безпеки підприємства. Також і нові технології можуть стати причиною інформаційної вразливості, якщо а) немає впевненості у їх надійності; б) відсутня належна кваліфікація для роботи із новими системами й технологіями. Так, незабезпечені патчами вразливості системи безпеки можуть бути використані для вторгнення зловмисників. Разом із тим надмірне зловживання технологіями захисту потребує значних ресурсів і знижує швидкодію й ефективність системи.

Так, потенційні клієнти дуже ймовірно покинуть сайт компанії, де для доступу до будь якої інформації слід буде реєструватись, проходити аутентифікацію тощо. подібне також частково можна описати і як наспупний пункт.

- Процеси та процедури: Неадекватні процеси та процедури, що регулюють доступ до інформації, можуть створювати ризики для її безпеки. Наприклад, якщо не існує контролю за доступом до чутливої інформації, це може привести до її втрати або пошкодження. Способів організації інформаційної взаємодії із клієнтами сьогодні існує безліч: це можуть бути прямі очні або телефонні контакти, електронна пошта, соціальні мережі, розсилки та фідбеки, численні месенджери тощо. Кожен із способів має свої переваги та недоліки і підібрати оптимальну процедуру для взаємодії із клієнтами та партнерами часто буває непросто, адже різні люди можуть мати свої об’єктивні та суб’єктивні схильності.

- Законодавство: законодавство, яке регулює захист інформації, може мати значний вплив на інформаційну безпеку підприємства. Ці впливи можуть залежати навіть від законів кількох держав, якщо підприємство має клієнтів/партнерів за межами країни. Наприклад, недотримання вимог законодавства про захист персональних даних може призвести до штрафів та інших правових наслідків. В Україні діє Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (опублікований у ВВР, 1994, № 31, ст.286, останні на момент написання даної роботи зміни внесено Законом № 2130-IX від 15.03.2022). Крім того, поводження із інформацію регулюють інші закони та підзаконні акти, наприклад такі, як ЗУ "Про захист персональних даних" (ВВР, 2010, № 34, ст. 481).

- Фізичне забезпечення та поводження з інформацією: Фізичний доступ до інформації також може становити загрозу її безпеці. Це загублені телефони чи ідентифікаційні картки, викрадення комп'ютерів або злам фізичних бар’єрів, підключення до захищених телефонних ліній тощо. Усе це може призвести до втрати конфіденційної інформації, розкриття даних, котре

впливатиме як на імідж самої компанії, так і торкатиметься інтересів окремих її кореспондентів.

- Зовнішні загрози: група чинників, деякі із яких частково зачеплені пунктами вище. Традиційно до групи зовнішніх загроз інформаційні безпеці підприємства відносять такі такі явища і процеси як хакерські атаки, фішинг, віруси і шкідливі програми, кібершпигунство й кібертероризм, незаконні прояви соціальної інженерії, тощо. Що цікаво, ця група чинників, якби аналіз було виконано 10, 20 чи 30 років тому, відрізнялась би кардинально, хоча зовнішні загрози інформаційній безпеці підприємства були основними ще задовно до розвитку Інтернет.

Відповідно структура, форми і види зовнішніх загроз інформаційній безпеці підприємства ще через якихось 10-20 років можуть докорінно змінитись. Визначимо сьогоднішній стан зовнішніх загроз в ТОВ «Глобал Вест», які можуть бути різного типу й походити з різних джерел. Основні зовнішні загрози для інформаційної безпеки підприємства включають:

– Хакерські атаки – це спроби зламування інформаційної системи підприємства з метою здобуття несанкціонованого доступу до конфіденційної інформації.

– Фішинг – це метод соціальної інженерії, коли зловмисник намагається отримати конфіденційну інформацію, використовуючи хитрість та маніпулювання щодо потенційної жертви. Переважно такі атаки розраховують на те, що користувачі будуть неуважними або недостатньо обізнаними із правилами поведінки у сучасних інформаційних системах, самостійно вводитимуть дані там, де це не передбачається.

– Віруси та шкідливі програми можуть завдати значної шкоди інформаційній системі підприємства, спричинити втрату даних або заблокувати доступ до них. Якщо йдеться про отримання доступу до цінних даних задля їх власного використання або продажу третій зацікавленій стороні, маємо кібершпигунство, якщо ж це робиться заради завдання прямої шкоди

підприємству або шантажування його розголошенням цих даних, це трактується як кібертероризм.

- Кібершпигунство – це збір конфіденційної інформації про підприємство з використанням інформаційних технологій.
- Кібертероризм – це використання комп'ютерних технологій для завдання шкоди підприємству з метою насильницького впливу на соціально-політичну ситуацію.

Зауважимо, що префікс «кібер-» говорить про нові форми роботи із даними, тоді як саме поняття шпигунства чи тероризування через розкриття інформації відомо задовго до кіберери: здавна викрадали плани й рецепти, робили компрометуючі знімки тощо.

– Соціальна інженерія – це метод, який заснований на маніпулюванні людьми з метою отримання доступу до конфіденційної інформації. Однією із найбільш небезпечних його форм є фішинг, проте загалом методи соціальної інженерії далеко ширші й заслуговують окремого дослідження

– Крадіжка ідентифікаторів, таких як паролі, може призвести до несанкціонованого доступу до чутливого контенту.

Таким чином, інформаційна безпека організації є надзвичайно важливим аспектом її діяльності. У сучасному цифровому світі, де дані є найціннішим активом, організації повинні приділяти належну увагу захисту своєї інформації від несанкціонованого доступу, втрати, викрадення або пошкодження.

У світлі постійного розвитку технологій та зростання кіберзагроз, організаціям необхідно бути постійно підготовленими до викликів, пов'язаних з інформаційною безпекою. Це означає впровадження оновлюваних стратегій та політик безпеки, регулярне оновлення програмного забезпечення та застосування передових методів захисту, а також постійне навчання персоналу щодо безпеки та свідомої поведінки в онлайн-середовищі.

Висновки до першого розділу

Інформація відіграє важливу роль у діяльності організації. Інформація – поняття загальне і багатоаспектне, воно пов’язано із передачею повідомлень від джерела до адресата. Для кількісного аналізу кількості інформації використовують імовірністні методи підрахунку.

Систему, котра оперує інформацією, збираючи, перетворюючи, передаючи та використовуючи іншим чином інформацію, називають інформаційною системою. Якщо таке оперування здійснюється із застосуванням технічних засобів, говорять про автоматизовану інформаційну систему. Технології, які використовують для роботи з інформацією, носять назву інформаційних технологій.

Серед компонент інформаційних систем та методів інформаційних технологій важливу роль відіграють компоненти та методи, які використовують для забезпечення інформаційної безпеки. Вони охоплюють системи шифрування даних, ідентифікації і аутентифікації користувачів, захищені канали та пристрої тощо.

На інформаційну безпеку підприємства впливають: люди, технології, процеси та процедури поводження з інформацією, законодавство, фізичне забезпечення інформаційної підтримки підприємства, а також зовнішні загрози.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОВ «ГЛОБАЛ ВЕСТ»

2.1 Чинники, що впливають на інформаційну безпеку ТОВ «Глобал Вест»

З 2004 року діє Товариство з обмеженою відповідальністю «Глобал Вест», яке було зареєстровано того року у Львові із статутним капіталом 23,7 тис. грн. Протягом часу діяльності це підприємство декілька разів змінювало чисельність працівників; спеціалізацію і напрям діяльності, проте його основним видом діяльності залишається неспеціалізована оптова торгівля, а додатковими виробництво будівельних виробів, складська діяльність тощо. Насправді спеціалізації у торгівлі вузьким спектром товарів та послуг є фактором конкурентної переваги, адже вузька ніша діяльності дає змогу за рахунок спеціалізації підвищити ефективність надання послуг чи поводження із товарами, проте така ринкова стратегія робить підприємство вразливим до змін ринкового середовища, яких за останній період було декілька, зокрема агресія 2014 року, пандемії та військове вторгнення в Україну 2022 року. Серед іншого, об’єктами, на торгівлі якими була сконцентрована діяльність підприємства, тривалий час, до 2022 року були пластикові віконні профілі, а також дверні системи виробника Open Teck – перший віконний профіль, виробництво якого цілком було організовано в Україні, а реалізація проводилась передусім у Києві, Харкові, Одесі та Дніпрі. Підприємство ТОВ «Глобал Вест» займалось дистрибуцією цієї продукції у західному регіоні України та наданням супутніх послуг. На жаль, основні потужності виробництва було розташовано у Новій Каховці, яка була окупована російськими військами ще 24 лютого 2022 року. Тому з початком збройної агресії підприємство ще деякий час реалізовувало складські запаси й далі знову змушене змінювати цільовий об’єкт спеціалізації. Зазначимо, що до 2012 року підприємство серед іншого здійснювало діяльність товарами широкого асортименту, у тому числі металевими й дерев’яними виробами, станками й

верстатами для їх обробітку, виробами із пластмас, у тому числі трубами, листами, в основному концентруючись на будівельних матеріалах.

Специфіка діяльності компанії визначає особливості її інформаційної безпеки. Як було зазначено у підрозділі 1.3, на інформаційну безпеку підприємства впливають передусім люди, технології, процеси, законодавство, фізичне забезпечення та інші внутрішні й зовнішні чинники. Розглянемо їхній вплив детальніше.

Вплив людського фактору на забезпечення інформаційної безпеки організації є вирішальним. При цьому доцільно розділити цю проблему на три складові:

1. Вплив на інформаційну безпеку ТОВ «Глобал Вест» з боку її працівників;
2. Вплив на інформаційну безпеку ТОВ «Глобал Вест» її партнерів і клієнтів;
3. Вплив на інформаційну безпеку ТОВ «Глобал Вест» третіх сторін.

Перший випадок найбільш важливий та критичний. Саме від обізнаності та відповідальності працівників залежить безпека компанії, організації чи підприємства. Хоча більшість підприємств забезпечують свої системи захисту паролями та іншими технічними засобами, але людський фактор є основною причиною порушення інформаційної безпеки. Недосвідченість та недбалість персоналу нерідко стає проблемою. Люди можуть ненавмисно створити проблеми для інформаційної безпеки підприємства, якщо вони не знають, які дії можуть призвести до порушень. Часто люди не приділяють належної уваги заходам безпеки та не слідкують за власними діями, що може призвести до порушень безпеки. Недостатня підготовка персоналу є суттєвим факторм ризику: кадри підприємства повинні бути добре підготовлені, щоб допомогти забезпечити безпеку даних та інформації у фірмі. Цей чинник варто розглянути більш детально у наступному підрозділі при розробці механізмів захисту даних та підвищення рівня інформаційної безпеки підприємства.

Поведінка партнерів може значно впливати на інформаційну безпеку фірми або організації, адже принаймні деяка частина інформації у підприємства й його партнерів є спільною. Ось деякі з можливих сценаріїв такого впливу: якщо партнери фірми не дотримуються належних процедур обробки та зберігання даних, це може призвести до витоку конфіденційної інформації або втрати даних; якщо партнери фірми не захищають свою мережу і інформацію від кібератак, це може стати причиною інцидентів безпеки, що можуть поширитися на фірму або організацію (наприклад, у фірми-партнера може бути список із контактами та даними працівників нашої фірми); незаконне використання даних – якщо партнери використовують конфіденційну інформацію фірми без дозволу або використовують її для особистої користі, це може призвести до серйозних наслідків для безпеки даних; якщо партнери фірми мають фінансові проблеми або заборгованості, це може призвести до того, що вони не зможуть забезпечувати належний рівень безпеки своїх систем і даних з об'єктивних причин, але нашій фірмі від того не легше; якщо партнери фірми не забезпечують достатньої освіти своїх співробітників про соціальну інженерію і фішинг, це може призвести до того, що зловмисники зможуть отримати доступ до систем фірми або організації.

Усі ці фактори можуть стати причиною ризику для інформаційної безпеки фірми або організації, тому важливо бути обережними при виборі та співпраці з партнерами і забезпечувати додаткові заходи безпеки (наприклад обмеження обміну даними), якщо є сумніви щодо дотримання партнерами регламенту поводження із конфіденційною інформацією.

Конфіденційна інформація – це інформація, яка повинна бути збережена в таємниці або обмеженому колі осіб, які мають доступ до неї. Це може бути будь-яка інформація, що містить приватні дані про особу, компанію, угоди, фінансову інформацію, торговельну таємницю, патентну інформацію, медичну інформацію та інше. Загалом конфіденційна інформація може бути зберігатися в будь-якому форматі: на папері, електронною поштою, на комп'ютері, в базі даних або на іншому носії інформації. Збереження конфіденційної інформації – це важливий

аспект інформаційної безпеки, оскільки доступ до такої інформації може бути обмежений або контрольований.

Зберігання та обробка конфіденційної інформації повинна відповідати вимогам законодавства та політики організації, яка зберігає таку інформацію. Крім того, доступ до конфіденційної інформації повинен бути обмежений лише необхідним колом осіб, а також забезпечувати її безпеку від несанкціонованого доступу, витоку або пошкодження. Прикладом організації роботи із конфіденційною інформацією може бути використання шифрів обмеженого доступу, наприклад ДСК, ДСКОД, ЦТ та інші.

Шифр ДСК – це скорочення від "для службового користування". Це означає, що документ з таким шифром призначений для внутрішнього використання в організації і не підлягає розголошенню або передачі третім особам без попереднього дозволу відповідної служби або керівництва організації.

Цей шифр може використовуватися на документах різного типу, таких як листи, накази, протоколи, звіти тощо, і позначається зазвичай в правому верхньому куті документа. Також існує інший шифр "Для службового користування з обмеженим доступом" (ДСКОД), який вказує на те, що документ містить конфіденційну інформацію і може бути доступний лише обмеженому колу осіб відповідно до встановлених процедур збереження конфіденційної інформації. Звісно, усі працівники організації повинні бути ознайомлені із недопустимістю розкриття інформації із документів з таким шифром стороннім особам та знати про відповідальність за таке розголошення. Документи з відповідними шифрами повинні зберігатись та поширюватись таким способом, що виключає їх контакт із випадковими сторонніми особами.

Діяльність підприємства ТОВ Глобал Вест не пов’язана із використанням інформації, що становить державну таємницю, проте окремі аспекти діяльності діяльності підприємства пов’язані з обробкою інформації, що містить комерційну таємницю, а тому потребують захисту від несанкціонованого втручання.

Державна таємниця та комерційна таємниця – це два різні типи таємниць, що мають свої особливості. Державна таємниця – це інформація, яка міститься в

документах, матеріалах, об'єктах або в електронних форматах, яка становить державну таємницю відповідно до законодавства про державну таємницю. Ця інформація стосується національної безпеки, оборони країни, зовнішньої політики, економіки, науки та техніки, культури тощо. Доступ до цієї інформації обмежується та регулюється законодавством. Розголошення державної таємниці може мати серйозні наслідки для національної безпеки та захисту державного суверенітету. Комерційна таємниця – це інформація, яка містить конфіденційні деталі про продукти або послуги, які створюються або надаються підприємством, а також інформація про бізнес-процеси та плани розвитку компанії. Ця інформація вважається конфіденційною та приховується від конкурентів та загального доступу. Розголошення комерційної таємниці може призвести до серйозних фінансових втрат та інших негативних наслідків для підприємства. З іншого боку, для компаній-конкурентів доступ до комерційної таємниці дуже бажаний. Крім того, існують ще такі види таємниць: професійна (як от лікарська або медична, адвокатська чи юридична), банківська – інформація про фінансові активи клієнтів. Особливий вид таємниці становить інтелектуальна власність (інформація, що містить результати творчої діяльності, які захищаються законодавством).

Третя складова впливу людського чинника на інформаційну безпеку пов'язана із діяльністю третіх сторін, тобто не працівників підприємства та не його безпосередніх партнерів. Деякі джерела виносять цей чинник (чинники) у окрему групу впливів, а серед людського чинника розглядають лише наслідки дій людей, що не мають наміру завдати шкоди підприємству чи організації.

У цій групі доцільно виокремити вплив двох підгруп: конкурентів та зловмисників, хоча у деяких випадках це може бути як одне, так і інше, а у деяких, доволі рідких випадках, шкода може бути пов'язана із діями випадкових осіб (наприклад, випадковий перехожий виклав у мережу селфі, де у кадр попав фрагмент підприємства чи його діяльності, який не хотілося б афішувати).

На ринку західного регіону України також присутні інші компанії-конкуренти, які займаються поширенням вікон, такі як «ЕКОвінд», ТОВ

Компанія «Грифон», «Євроком», «Елегант», ПНВП «Корпускула», «Фабрика Вікон», Віконна компанія «Піраміда», «Нове вікно», ТОВ "Термопласт плюс", тощо. Кожна з цих компаній пропонує свої послуги і конкурує на ринку віконного бізнесу.

Розглянемо потенційні наслідки дій конкурентів ТОВ «Глобал Вест» у сфері, які шкодять її інформаційній безпеці.

Традиційно роль конкурентів може бути зведена до одного із кількох сценаріїв:

- Конкуренти отримують доступ до розробок компанії й використовують їх у своїй діяльності, економлячи кошти на власних дослідженнях й підриваючи конкурентну перевагу фірми.
- Конкуренти отримують доступ до планів компанії (перелік потенційних клієнтів, графік поставок сировини та продукції, зміст конкурентних заявок на тендерах тощо) і можуть перешкодити їх реалізації (переманити клієнтів, організувати поставки своєї продукції на локальні ринки таким чином, щоб вона з’явилась трохи раніше, подати конкуруючу заявку за ціною на 1 грн нижчою і т.п.).
- Конкуренти провадять інформаційну боротьбу з метою дискредитувати організацію, причому підстави можуть бути не обов’язково пов’язані із якістю послуг та товарів компанії: можуть стосуватись її зв’язку із фінансовими установами або постачальниками, що себе дискредитували, або ж етичних аспектів поведінки керівництва компанії чи її працівників тощо (т.зв. чорний піар). В умовах поширених соціальних мереж організувати подібну компанію зазвичай не складно, хоча її ефективність може бути сумнівною, або навіть може мати ефект бумеранга.

Інформаційна безпека є дуже важливим фактором в конкурентній боротьбі на ринку. Конкурентність між підприємствами веде до постійної роботи над новими ідеями, розробками та інноваціями, що потребує обміну конфіденційною інформацією. Захист цієї інформації є важливою складовою успіху на ринку. Інформаційна безпека забезпечує захист від крадіжки конфіденційної

інформації, що може призвести до відтворення чи підробки продукту чи послуги конкурента. Крім того, безпека даних допомагає зберегти конкурентну перевагу, зберігаючи унікальні знання та ноу-хау компанії в таємниці. Інформаційна безпека також забезпечує захист від шпигунства та крадіжки інтелектуальної власності (див далі), такої як патенти, авторські права і торгові марки. Захист інформації також допомагає зберегти репутацію компанії та захистити клієнтів від можливої крадіжки їхніх даних.

Отже, інформаційна безпека ТОВ «Глобал Вест» є надзвичайно важливим аспектом в конкурентній боротьбі на ринку. Забезпечення безпеки інформації допомагає захистити конфіденційну інформацію, зберегти конкурентну перевагу, захистити інтелектуальну власність і зберегти репутацію компанії.

Нарешті остання підгрупа чинників людського фактору, що впливають на інформаційну безпеку компанії, пов’язана із діями зловмисників, що не є прямими конкурентами компанії. Йдеться передусім про хакерську діяльність.

Хакери та інші зловмисники можуть використовувати соціальну інженерію, щоб отримати доступ до ідентифікаторів користувачів, таких як паролі. Користувачі повинні бути обережними, щоб не допустити крадіжки своїх ідентифікаторів та паролів. Отримавши доступ до конфіденційної інформації про компанію хакери можуть: – вимагати викуп за її нерознолошення; – продати її конкурентам (див. попередній пункт); – розкрити її завдавши шкоди іміджу компанії (навіть якщо там немає жодних відомостей, що дозволяють у негативному ключі говорити про компанію, сам факт витоку інформації свідчить, що підприємство недостатньо дбає про безпеку, а тому з ним краще не мати справ).

Викрадення даних клієнтів може дуже серйозно пошкодити інформаційну безпеку підприємства. Клієнтська інформація, така як імена, адреси, номери телефонів, адреси електронної пошти, інформація про кредитні картки, інші фінансові дані та особисті дані можуть бути використані зловмисниками для кібератак на клієнтів підприємства, включаючи фішинг та ідентифікаційні шахрайства. Для прикладу, за даними групи Data1eaks (телеграм-канал https://t.me/data 1eaks) від 8/5/23 проросійська група "XakNet Team" здійснила злом страхової

компанії "Оранта" і отримала доступ до 12,5 млн записів про особу клієнтів (ім'я, дата народження, стать, адреса реєстрації) та майже 7 млн записів про автомобілі (VIN, ДРЗ, марка/модель, регіон/місто), актуальність викраденої бази даних – грудень 2022 року. Такі витоки інформації, особливо у західному світі, вкрай негативно відображаються на репутації компанії.

Крім того, якщо зловмисники отримують доступ до інформації про клієнтів, вони можуть використовувати цю інформацію для випадкової або цілеспрямованої атаки на саме підприємство. Вони можуть використовувати отриману інформацію для зламу систем безпеки, отримання несанкціонованого доступу до інформації, вимагання викупу зашифрованої інформації, або використати її для розробки нових видів кіберзлочинності.

Отже, викрадення даних клієнтів може привести до серйозного порушення інформаційної безпеки підприємства, втрати довіри клієнтів та фінансових втрат. Організації повинні вживати всіх можливих заходів для захисту даних клієнтів, включаючи використання ефективних заходів забезпечення безпеки, таких як шифрування, регулярні оновлення програмного забезпечення та навчання персоналу з питань кібербезпеки.

Інший можливий наслідок дій хакерів – знищення даних, порушення нормального функціонування систем тощо. Причинами можуть бути як хуліганські наміри, так і замовлення з боку конкурентів і/або ідеологічна незгода з політикою чи діяльністю компанії. Найбільш відома (проте лише одна із багатьох) форма таких атак – т.зв. DDoS атака, коли унаслідок надмірної кількості запитів із мережі сайт компанії не працює або працює із перебоями. Численні атаки такого типу спостерігались на систему банків України весною 2022 року.

У контексті аналізу стану інформаційної захищеності ТОВ «Глобал Вест» проведемо вивчення доступної із відкритих джерел аналізу інформації. Пошук за ключовою фразою, пов'язаною із підприємства проведено у основних пошукових платформах. Результати подано у таблиці 2.1.

Таблиця 2.1.

Результати пошуку інформації про підприємство у відкритих джерелах

Пошукова система (ПС)	Популярність ПС в Україні станом на 2021 р.	Кількість результатів		Домени результатів, що перші у пошуку результати
		точна фраза "ТОВ Глобал Вест"	точна фраза "Глобал Вест"	
Google	92.2%	105	5 920	youcontrol.com.ua/ opendatabot.ua/ www.ukraine.com.ua/ clarity-project.info/ okna.ua/ua/globalwest list.in.ua/ nomis.com.ua/ odnodata.com/ 5140.org/
Bing	2.27%	1 130	23 200	opendatabot.ua/ leadscanner.com.ua/ edr-info.com/ nomis.com.ua/ clarity-project.info/ okna.ua/ua/globalwest **global-west.business-guide.com.ua/**
Yahoo!	1.5%	1 080	15 300	opendatabot.ua/ leadscanner.com.ua/ edr-info.com/ nomis.com.ua/ okna.ua/ua/globalwest
Baidu	1.45%	15+	15+	www.bilibili.com/ www.kuwo.cn/ v-wb.youku.com/
Yandex	0.68%	*не доступно*		
DuckDuckGo	0.59%	21	44	opendatabot.ua/ leadscanner.com.ua/ edr-info.com/ www.dlab.com.ua/ www.ua-region.com.ua/ clarity-project.info/ www.ukraine.com.ua/

Проведено пошук інформації, асоційованої із назвою компанії, у шести найбільш популярних (за даними статистики) пошукових системах. Зауважимо, наступне: пошук по Яндекс наразі недоступний, пошук по китайській пошуковій системі Baidu дає нерелевантні результати; із решту чотирьох пошукових систем, кожна з яких має свої алгоритми пошуку та власні бази даних, безпосередньо сайт підприємства знайдено лише за допомогою пошукової системи Bing; у інших пошукових системах на кількох перших сторінках цей сайт не відображається. Така інформація може свідчити про недостатній рівень інформаційної діяльності компанії у мережі інтернет та потребу працювання над донесенням можливостей компанії у шикокої маси споживачів. Знайдений сайт https://global-west.business-

guide.com.ua/ розміщено на порталі «Бізнес-Гід» і оформлено так, як показано на рис.2.2.

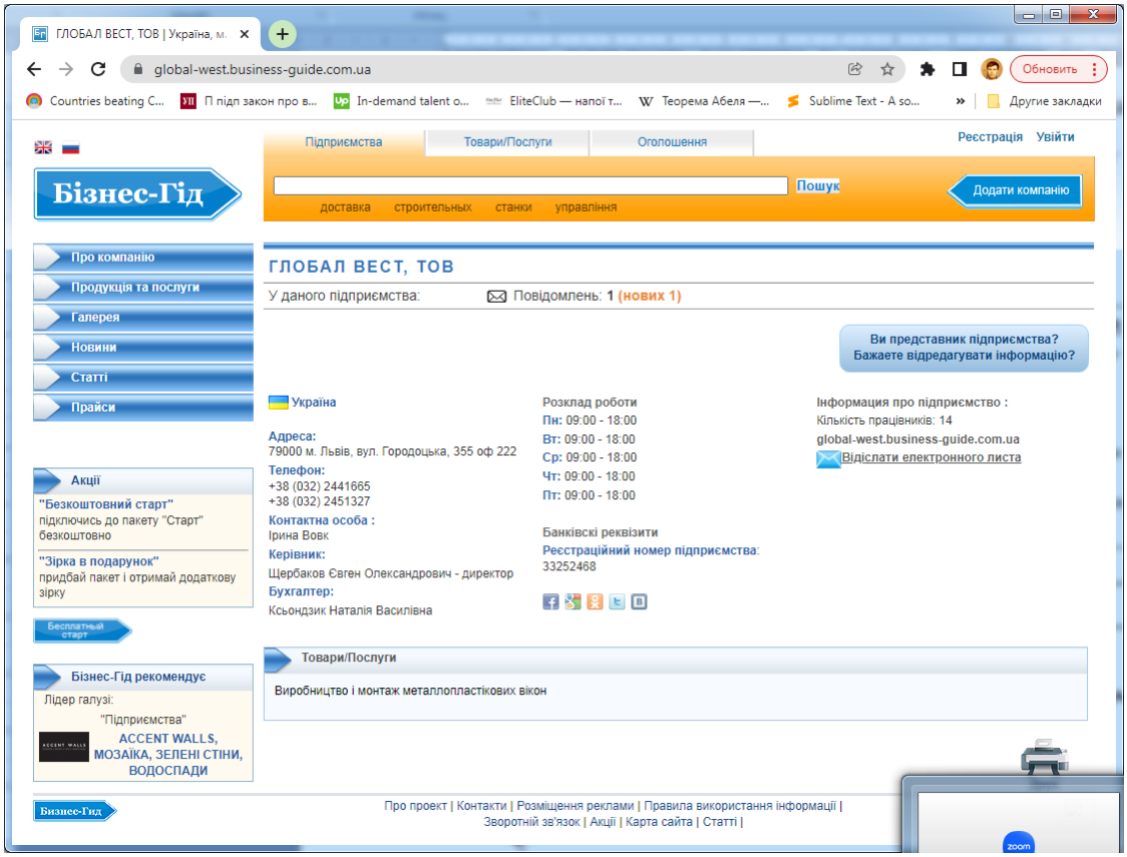

Рис.2.2. Сайт підприємства

Зауважимо, що дані, присутні на цьому сайті, дуже важливі з огляду на інформаційну безпеку підприємства, адже із такої інформації переважно зловмисники можуть розпочинати інформаційну кампанію проти підприємства. Тут вказано загальну інформацію про підприємство, а саме: кількість працівників (14), реєстраційний номер підприємства (33252468), розклад роботи (стандартний, кожен робочий день із 9:00 до 18:00), адреса (79000 м. Львів, вул. Городоцька, 355 оф 222), телефони (+38 (032) 2441665, +38 (032) 2451327), а також прізвища та імена кількох осіб:

– контактна особа
– керівник підприємства (директор) та
– бухгалтер

Дані цих осіб можна в подальшому використати для пошуку конфіденційної інформації у соціальних мережах та застосування інших інструментів соціальної інженерії для отримання доступу до інформації про підприємство. Тому з міркувань інформаційної безпеки слід передусім дбати про інформаційну гігієну саме цим особам: профіль у соціальних мережах тримати закритим, відповідально ставитись до збереження надійних паролів для доступу до пошти та різних сервісів, використовувати різні номери телефону для особистих та службових потреб тощо.

Захист від атак може включати в себе такі заходи, як використання сильних паролів, не відкривання сумнівних посилань, використання антивірусного програмного забезпечення та захисту від шпигунського програмного забезпечення. Крім того, важливо вчити людей бути обережними зі своїми персональними даними та навчати їх ідентифікувати підозрілі повідомлення та дії в Інтернеті. Адже зловмисники можуть використовувати різноманітні техніки, щоб отримати доступ до конфіденційної інформації, використовуючи персональні дані людей, наприклад: фішинг: відправляти електронні листи, які виглядають як повідомлення від різних організацій (наприклад, банків, соціальних мереж, інтернет-магазинів) з проханням надати свої персональні дані, такі як логіни, паролі, номери кредитних карток. Якщо людина відправляє ці дані зловмисникам, вони можуть використовувати їх для отримання доступу до конфіденційної інформації; соціальний інжиніринг: зловмисники можуть використовувати соціальний інжиніринг, щоб отримати доступ до конфіденційної інформації (наприклад, використовувати соціальні мережі для отримання персональних даних про людей, таких як місце роботи, місце проживання, інтереси та інше. Після цього вони можуть використовувати ці дані для того, щоб переконати людей надати доступ до конфіденційної інформації); віруси та шпигунське програмне забезпечення: зловмисники можуть використовувати віруси та шпигунське програмне забезпечення для отримання доступу до конфіденційної інформації.

2.2 Аналіз господарської діяльності ТОВ «Глобал Вест» та механізми дотримання інформаційної безпеки підприємства

Існують загальні принципи дотримання інформаційної безпеки підприємств та організацій і можуть бути особливості їх імплементації у практику діяльності конкретних структур із врахуванням специфіки діяльності. Механізми дотримання інформаційної безпеки ТОВ «Глобал Вест» включають такі елементи:

- Політика і процедури безпеки. Розроблення і впровадження політик і процедур, які визначають, які типи інформації потрібно захищати, які засоби захисту використовувати, які правила дотримуватися працівникам тощо. Політика безпеки – верхній управлінський рівень в організації , який визначає загальні підходи щодо інформаційної безпеки, у різних підрозділів. Важливим при цьому є дотримання загальних принципів та, за потреби, їх адаптація до локальних умов.
- Технічні засоби захисту. Встановлення у ТОВ «Глобал Вест» технічних засобів захисту, таких як антивірусне програмне забезпечення, брандмауери, захищені канали зв'язку, системи шифрування тощо. Наскільки має бути захищеним конкретний канал комунікації, залежить від каналу, суті інформації, для передачі якої він використовується, а також від політики компанії.
- Вміння та навики працівників у сфері дотримання безпеки. В організації регулярно проводяться тренінги з питань інформаційної безпеки в організації для підвищення рівня свідомості працівників щодо інформаційної безпеки та навчання їх правильній поведінці в мережі.
- Моніторинг і аудит. На ТОВ «Глобал Вест» проводиться регулярний моніторинг систем безпеки для виявлення можливих загроз та аналізу потенційних ризиків.
- Аварійне реагування. Розроблення планів дій у разі виявлення загроз та випадків порушення безпеки даних.

Важливо враховувати, що механізми дотримання інформаційної безпеки у ТОВ «Глобал Вест» є постійно оновлюваними та вдосконалюваними, оскільки загрози та ризики постійно змінюються та зростають.

Інформаційна безпека в організації є інтегрована у процеси господарської та організаційної діяльності ТОВ «Глобал Вест». Остання здійснюється на базі статуту організації законодавства України, включаючи, але не обмежуючись Конституцією України, законами, постановами Президента і Кабінету Міністрів України. Безпосередньо у статуті підприємства термін "інформаційна безпека" не згадується. Статут визначає як основну мету діяльності створення і отримання прибутку. Стратегія організації передбачає укладанян довгострокових і взаємовигідних відносин з клієнтами.

Основним видом діяльності ТОВ «Глобал Вест» згідно статуту та даних реєстрації є оптова неспеціалізована торгівля. У сфері оптової торгівлі інформаційна безпека є важливою, адже підприємства мають велику кількість даних, пов’язаних з клієнтами, постачальниками та іншими бізнес-партнерами. Характерними рисами інформаційної безпеки у сфері оптової неспеціалізованої торгівлі є: збільшена кількість інформації – підприємства отримують велику кількість інформації від клієнтів і постачальників, що потребує ефективного контролю за її збереженням і захистом; ризики взаємодії з багатьма бізнес-партнерами – підприємства мають багато бізнес-партнерів, з якими потрібно обмінюватися інформацією, що створює додаткові ризики викрадення даних та зламів; збільшення ризику кібератак – збільшена кількість інформації і бізнес-партнерів збільшує ризики кібератак, які можуть призвести до втрати даних та порушення конфіденційності. Тому важливо розробляти та впроваджувати ефективні механізми забезпечення інформаційної безпеки у сфері оптової торгівлі для захисту від можливих загроз і збереження довіри клієнтів.

ТОВ «Глобал Вест» реалізує широкий асортимент товарів, у тому числі профільні системи, будівельні матеріали, виконує посередницьку діяльність у торгівлі широкого профілю, тому повинна мати справу із клієнтами також широкого профілю. Налаштування інформаційних систем підприємства на ро-

боту із широким спектром клієнтів потребує значних зусиль загалом та у сфері забезпечення інформаційної безпеки, адже фахівці відділу продажів мають бути готові допомогти клієнту із замовленням різної складності, а тому інформаційна система має бути достатньо універсальна, масштабована, а такі системи потребують підключення компонент, які можуть негативно відобразитись на безпеці системи.

Тим не менш деякі елементи фінансової звітності можна знайти із відкритих джерел у інтернету. Так, на домені Opendatabot за інтернет-адресою https://opendatabot.ua/c/33252468 можна знайти дані про дохід, чистий прибуток, активи і зобов'язання Товариства з обмеженою відповідальністю «Глобал Вест» за 2020, 2021, 2022 роки, у тому числі дані, що можуть сформувати негативне уявлення про стан діяльності підприємства, оскільки упродовж цих років у компації фіксували від'ємний чистий прибуток. Ці дані показано у таблиці 2.2.

Таблиця 2.2.

Фінансова звітність ТОВ «Глобал Вест»*

	2022	2021	2020	2019
Дохід	755 600 грн	10 227 400 грн	5 557 700 грн	6 233 550
Чистий прибуток	–247 700 грн	–474 700 грн	–586 500 грн	-753 185
Активи	4 125 300 грн	6 051 200 грн	3 714 300 грн	3 988 255
Зобов'язання	3 395 500 грн	5 073 700 грн	0 грн	-

* Платник ПДВ, Номер свідоцтва – 332524613033, станом на: 02.03.2023

Від'ємний чистий прибуток у фінансовій звітності підприємства свідчить про те, що за останніх чотири роки підприємство зазнало збитків, тобто його витрати перевищили прибуток. Це може бути наслідком різних факторів, таких як зниження продажів, зростання витрат на виробництво чи послуги, збільшення податкових платежів, або низька ефективність управління фінансами.

Від'ємний чистий прибуток не завжди є ознакою того, що підприємство насправді працює неефективно. В деяких випадках, великі інвестиції в нові технології, розширення ринків, або інші довгострокові стратегії можуть призвести до від’ємного чистого прибутку, проте в подальшому забезпечити стабільний ріст і прибутковість підприємства.

Фінансовий стан підприємства з позицій короткострокові перспектив оцінюється показниками ліквідності (рис. 2.3) та платоспроможності. Загалом ці показники характеризують здатність підприємства вчасно і в повному обсязі здійснювати розрахунки за короткостроковими зобов’язаннями з контрагентами.

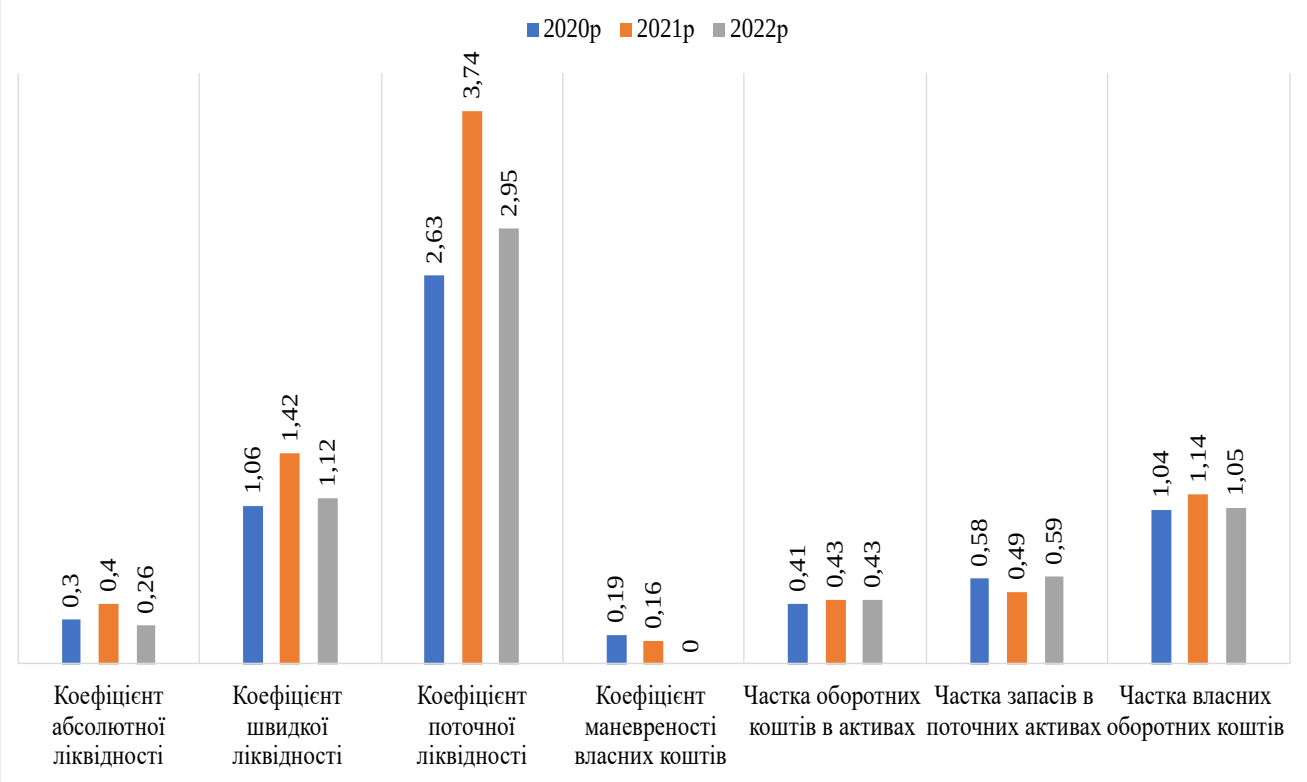

Рисунок 2.3. Характеристика показників ліквідності ТОВ «Глобал Вест»

Ступінь ліквідності визначається тривалістю часового періоду протягом якого ця трансформація може бути здійснена тобто чим коротший період вище ліквідність активів.

Якщо підприємство не може погасити свої поточні зобов’язання по мірі того як наступає термін їх оплати, подальший розвиток діяльності організації ставиться під сумнів.

Характеристика показників ліквідності ТОВ «Глобал Вест» (рис.2.3) дає можливість оцінити загальну ефективність інвестування коштів у дане підприємство. На відміну від інших показників, вони аналізують рентабельність капіталу в цілому. Таким чином, ми спостерігаємо, що розмір власного оборотного капіталу хоча і в невеликих масштабах, але зростає з року в рік. Товариство з обмеженою відповідальністю «Глобал Вест» не є збитковим і має можливості для функціонування та ефективного розвитку.

Аналізуючи рисунок 2.4, можна зробити висновок, що діяльність Товариства з обмеженою відповідальністю «Глобал Вест» залежить від позикових коштів. Для такої залежності характерна довготривала робота з проєктування та виготовлення готової продукції. Для свого виробництва компанія бере короткострокові кредити або залучає державні кошти.

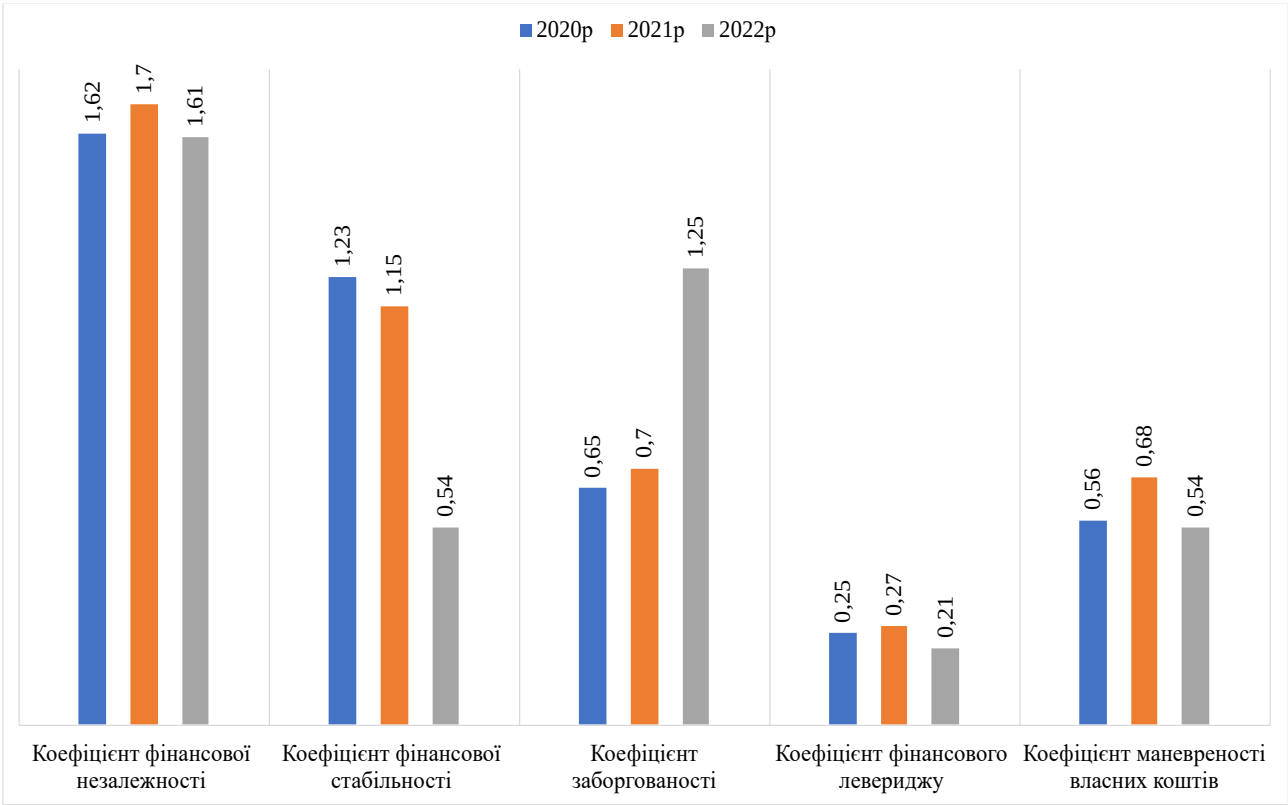

Рисунок 2.4 Характеристика фінансової стійкості ТОВ «Глобал Вест»

Інформаційна безпека ТОВ «Глобал Вест» пов’язана з його фінансовим станом. Негативний чистий прибуток свідчить про фінансові проблеми

підприємства, які неабияк впливають на його інформаційну безпеку. Наприклад, якщо підприємство має фінансові труднощі, то воно може зменшити інвестиції в захист інформації та технологічні засоби захисту. Хоча це може зробити його більш вразливим до кібератак та інших форм кіберзлочинності. Крім того, негативний фінансовий стан може призвести до погіршення якості обслуговування та підтримки користувачів, що також може вплинути на інформаційну безпеку підприємства. Отже, важливо, щоб підприємство відводило достатньо коштів на захист інформації та інвестувало у сучасні технології та методи захисту.

У Товаристві з обмеженою відповідальністю «Глобал Вест» завдяки високошвидкісному Інтернет-зв'язку та сучасній трудовій етиці дозволяється офісним працівникам частину роботи виконувати з дому, тобто робота у змішаному форматі. Сьогодні такий режим роботи набуває популярності і є значною перевагою для ТОВ «Глобал Вест».

Для забезпечення безпеки, будь-які пристрої, що використовуються співробітниками чи клієнтами для віддаленого доступу до робочої мережі, відповідають нормам інформаційної безпеки.

На підприємстві ТОВ «Глобал Вест» застосовуються універсальні та масштабовані інформаційні системи (UMIS). Вони використовуються для обробки великого обсягу даних, що ставить питання про їхню інформаційну безпеку важливим завданням. Основні проблеми, які пов’язані з інформаційною безпекою UMIS, включають:

Доступ до даних. У зв’язку з великою кількістю користувачів та обсягом оброблюваних даних, важливо в організації ТОВ «Глобал Вест» забезпечити правильний доступ до даних відповідно до рівня дозволу та політики безпеки.

Забезпечення цілісності даних. У зв'язку з великою кількістю користувачів та обсягом даних, які оброблюються, в організації можливість порушення цілісності даних зростає. Тому важливо забезпечити належну захист від несанкціонованих змін даних.

Захист від вторгнень. Велика кількість користувачів та обсяг даних, що оброблюються, може зробити UMIS привабливим для хакерів. Тому важливо забезпечити належний рівень захисту від вторгнень та несанкціонованого доступу до системи.

Захист від зловживання правами доступу. Велика кількість користувачів та обсяг даних, які оброблюються, може створити загрозу від несанкціонованого використання прав доступу. Тому важливо забезпечити належний контроль за використанням прав доступу та політику безпеки.

Забезпечення безпеки мережі. Велика кількість користувачів та обсяг даних, що оброблюються, вимагає високої ступені захисту мережі від несанкціонованого доступу та зловживання правами доступу.

В організації ТОВ «Глобал Вест» група захисту від промислового шпигунства безпосередньо підпорядкована начальнику служби безпеки. Обов'язки начальника служби безпеки включають:

1. Розробка та впровадження політики інформаційної безпеки на підприємстві. У даному питання він взаємодіє із керівником та системним адміністратором та ініціює розгляд питань по суті.

2. Виявлення потенційних загроз для інформаційної безпеки та розробка заходів з їх запобігання. До виконання цих завдань можуть бути залучені експерти та сторонні фахівці. Нерідко деякі інформаційні послуги підприємство може замовити у третіх сторін (наприклад, розробку та підтримку сайтів; формування структури захищеної бази даних чи арендування її розміщення у хмарному сервісі)

3. Забезпечення дотримання вимог законодавства в галузі інформаційної безпеки. Якщо кваліфікація начальника служби безпеки дозволяє, цими питаннями він опікується особисто. У протилежному випадку – консультується із юридичним відділом.

4. Організація та проведення тренінгів та семінарів з питань інформаційної безпеки для співробітників підприємства. Сьогодні послуги із надання навчання комп'ютерній, у тому числі мережевій та інформаційній грамотності

надають численні фірми на ринку. Слід пам’ятати, що рівень викладання має бути адаптований під рівень знань працівників, що часто не є просто і тому працівники, стикаючись із фразами про симетричні і асиметричні методи захисту інформації можуть пройти таке навчання лише формально, що знижує його ефективність. У даному випадку оптимально було б стимулювати самоосвіту працівників, проте такі методи також не завжди працюють.

5. Встановлення та контроль за дотриманням правил доступу до конфіденційної інформації на підприємстві. Це і наступне основний напрям діяльності начальника служби безпеки на середньому підприємстві, при цьому він взаємодіє із начальниками відділів та узгоджує правила із керівником підприємства.

Контроль за роботою з інформаційними ресурсами підприємства та захистом їх від зловживань. Тут роль начальника служби безпеки переважно контролююча, основні завдання має виконати системний адміністратор, у тому числі налаштувати мережу, права доступу до пошти та спільних ресурсів. Тому у випадку підприємств із дійсно невеликим штатом може бути доцільно поєднати обов’язки адміністратора із начслужбезу.

Аналіз та оцінка ризиків в галузі інформаційної безпеки на підприємстві та вжиття заходів з їх зменшення. Тут зазвичай потрібна допомога аналітичного відділу, якщо такий існує на підприємстві. У протилежному випадку гарною ідеєю є періодичне обговорення ризиків інформаційної безпеки у ході мозгових штурмів при зустрічах різного складу та періодичності.

До обов’язків начальника служби безпеки входять інші завдання, залежно від конкретних потреб підприємства та розміру його служби безпеки.

Внутрішнє та зовнішнє середовище організації є важливими компонентами її конкурентоспроможності та інформаційної безпеки. Для здійснення аналізу цих середовищ у розрізі конкурентоспроможності ТОВ «Глобал Вест» переважно застосовують матрицю SWOT-аналізу (рис.2.5).

SWOT- дозволяє визначити сильні та слабкі сторони на підприємстві, а також можливості і загрози внутрішнього середовища, зокрема інформаційної безпеки організації.

Перевага в ресурсах і виробництва дозволяють ТОВ «Глобал Вест» пропонувати споживачам різноманітний асортимент продукції вищої якості за нижчими цінами, ніж у конкурентів, і таким чином досягти переваги. Досягнуті переваги дозволяють мати міцніші позиції на ринку, досягати показників прибутковості вище середньогалузевих, що в подальшому сприятиме подальшому розвитку сильних сторін організації та усуненню її слабких сторін.

Рис. 2.5 Матриця SWOT-аналізу ТОВ «Глобал Вест»

Інформаційна безпека внутрішнього середовища організації залежить від: культури безпеки ТОВ «Глобал Вест»: наявність внутрішньої культури безпеки є ключовим фактором для забезпечення інформаційної безпеки організації; продумана політика безпеки, свідомість працівників про загрози та правильна поведінка відносно інформаційної безпеки є важливими аспектами внутрішньої культури безпеки; кадровий потенціал: працівники організації є важливим елементом її інформаційної безпеки; належний підбір кадрів, їх професійне навчання та розвиток є необхідними для забезпечення безпеки інформації в організації; технічні засоби захисту: наявність і правильне використання технічних засобів захисту є важливими для забезпечення інформаційної безпеки внутрішнього середовища організації.

Зовнішнє середовище організації включає в себе всі зовнішні фактори, що впливають на інформаційну безпеку організації. Інформаційна безпека зовнішнього середовища організації включає заходи, спрямовані на захист інформації від небажаного доступу, втручання та впливу з боку зовнішніх загроз. До таких загроз можуть належати: дії зловмисників, які можуть намагатися отримати несанкціонований доступ до комп'ютерних систем організації, використовуючи різноманітні техніки, такі як віруси, троянські програми, фішинг, скімінг та інші; соціальний інжиніринг – зламування системи шляхом отримання доступу до важливої інформації через використання маніпулювання людьми, що працюють в організації; фізичні загрози – як от крадіжки комп'ютерної техніки, проникнення в приміщення організації для злому систем інформаційної безпеки, знищення документів та інші; шпигунство – вороги можуть намагатися отримати важливу інформацію про діяльність організації, щоб використовувати її в своїх цілях; складні мережі постачальників, багато організацій підприємницької діяльності мають складні мережі постачальників, іноземні і контрактні робітники. Кожен новий елемент мережі потенційно є джерелом проникнення й порушення інформаційної безпеки.

Виділимо основні зовнішні фактори, які впливають на діяльність організації. Їх можна розділити на три групи факторів, а саме перша група пов'язана зі збутом продукції, друга група – характеристика забезпечення нормальної роботи організації, сировина та інструменти, а третя група – характеристика системних параметрів, таких як стан економіки країни, податкове законодавство та інші види нормативних норм.

Таким чином аналіз інформаційного забезпечення ТОВ «Глобал Вест» вказує на недостатню захищеність інформаційної безпеки з боку персоналу. Адже ніколи неможливо на сто відсотків довіряти працівникам.

Механізми дотримання інформаційної безпеки ТОВ «Глобал Вест» розробляють й запроваджують із врахуванням аналізу ризиків інформаційної безпеки підприємства. Цей процес передбачає ідентифікацію потенційних загроз та вразливостей інформаційної інфраструктури підприємства, оцінку ймовірності виникнення загроз та наслідків їх реалізації, а також визначення заходів щодо запобігання та мінімізації наслідків таких загроз.

Після проведення аналізу ризиків підприємство може розробити стратегію забезпечення інформаційної безпеки, включаючи заходи щодо запобігання загрозам та мінімізації наслідків їх реалізації. Основні системні зміни вимагають ретельної оцінки ризиків для визначення нових вимог безпеки.

Ефективна програма управління ризиками повинна забезпечувати досягнення бізнес-цілей організації шляхом: більш ефективного захисту інформаційної безпеки в організації, які зберігають, обробляють і передають інформацію, що належить ТОВ «Глобал Вест», дозволяючи керівництву обґрунтовувати свої рішення щодо бюджетних витрат на управління ризиками. Нами сформовано модель управління інформаційними ризиками ТОВ «Глобал Вест» (рис.2.6), яка допоможе виокремити два основні процеси уникнення загроз та послаблення ризику: оцінка ризику та пом'якшення ризику.

Оцінка ризику включає: виявлення та визначення вартості активів організації – тут може бути використаний якісний або кількісний метод, виявлення загроз та визначення ймовірності їх виникнення, аналіз ризиків –

оцінка сприйнятливості систем або активів до виникнення факторів ризику (фактори ризику, що сприяють виникненню збитків). Зменшення ризику складається з таких дій: вибір відповідних механізмів безпеки, впровадження, тестування та моніторинг механізмів безпеки, прийняття залишкового ризику.

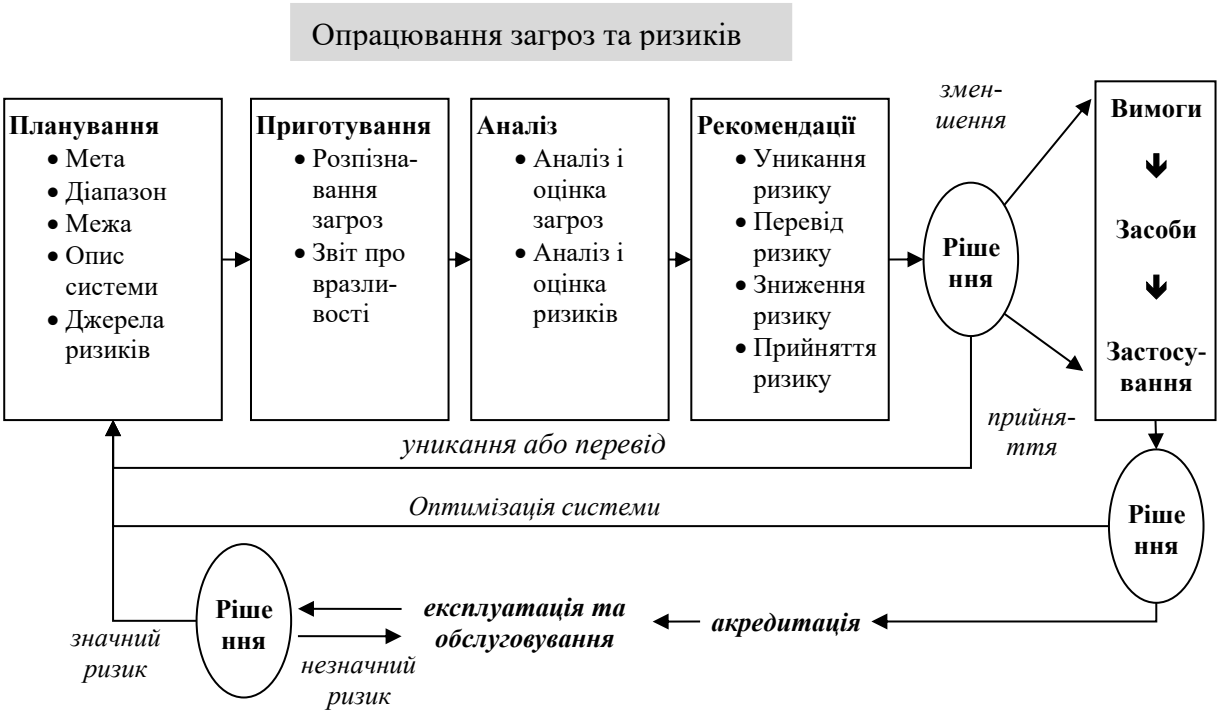

Рис.2.6. Модель управління інформаційними ризиками ТОВ «Глобал Вест»

Таким чином, аналізуючи реакцію системи на ризики, бачимо декілька варіантів дій, які не заперечують, але доповнюють один одного: звісно, ризиків інформаційної безпеки слід уникати, проте не усі ризики можуть бути виключені навіть у ідеальній системі. Тому й існують механізми перенесення, зменшення наслідків та прийняття ризику.

2.3 Пропозиції для підвищення рівня інформаційної безпеки ТОВ «Глобал Вест»

Для того щоб не стати жертвою кібер злочинців керівництво ТОВ «Глобал Вест» приділяє увагу захисту даних. Однак інструменти кіберзлочинців

удосконалюються, а підприємці не завжди встигають прослідковувати за змінами. Саме тому, ми пропонуємо дотримання наступних правил (рис.2.7):

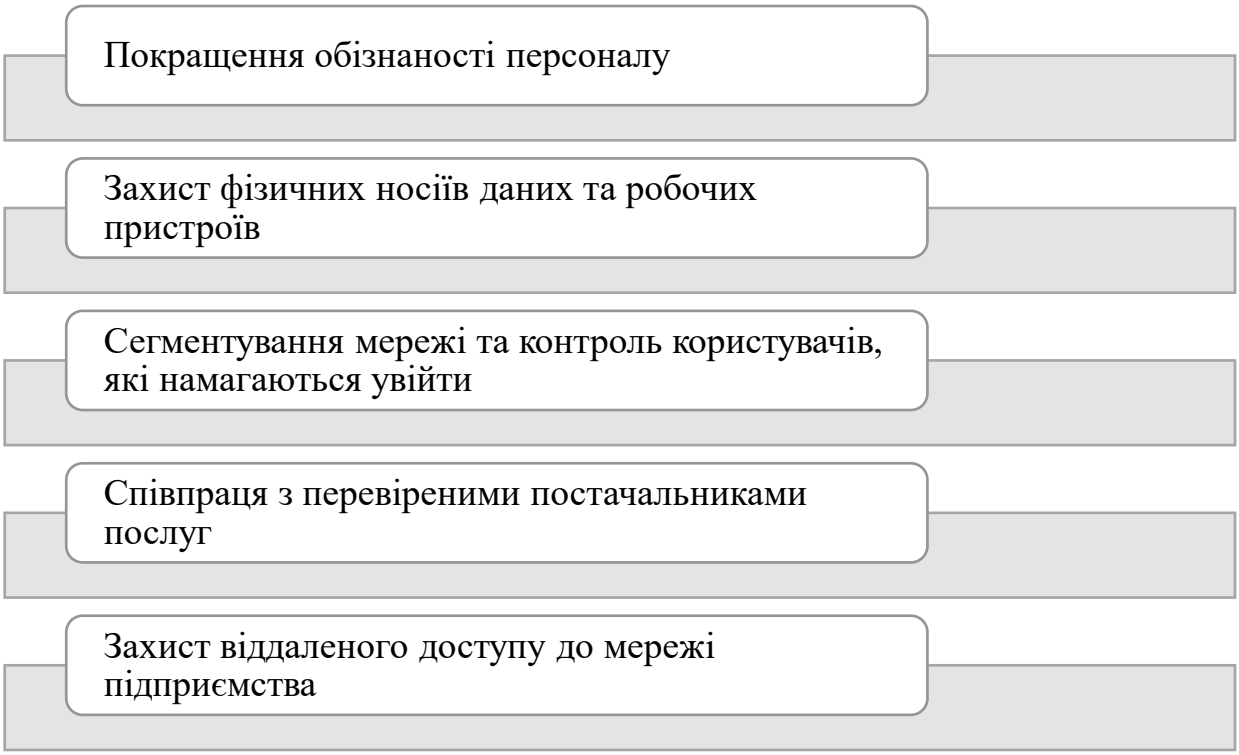

Рис.2.7 Правила дотримання необхідного забезпечення інформаційної безпеки ТОВ «Глобал Вест»

Важливо наголосити, що кіберзлочинці зазвичай використовують недосвідчений персонал як «найслабше місце» в компанії для отримання доступу до корпоративних даних. Це здійснюється шляхом надсилання фішингових повідомлень, які є дуже реалістичними, та змушують співробітників відкривати їх. Наслідком може бути завантаження на пристрій шкідливих програм, таких як вимагачі, трояни, шпигунське програмне забезпечення та інше шкідливе програмне забезпечення.

Тому першим і найважливішим кроком у забезпеченні інформаційної безпеки компанії є належне навчання та інформування персоналу про поточні загрози та методи захисту. Кожен працівник повинен розуміти важливість захисту даних компанії та її клієнтів.

Для забезпечення безпеки компанії необхідно проводити регулярні навчання співробітників щодо актуальних загроз і методів захисту. Це повинно

охоплювати ознайомлення з фішинговими атаками, розпізнавання підозрілих повідомлень та поведінки в Інтернеті. Крім того, пропонується використовувати рішення для шифрування даних, регулярно робити резервне копіювання та встановлювати актуальні антивірусні програми.

Сегментування корпоративної мереж переважає у зниженні навантаження на систему та контролі доступу та підвищення інформаційної безпеки. В контексті інформаційної безпеки, конфіденційні дані слід розміщувати на окремих серверах, забезпечуючи їх додатковий захист за допомогою брандмаузерів або інших служб безпеки. Це створює багато бар'єрів, котрі зберігають дані та допомагають знизити ризик їх втрати. Крім того, необхідно моніторити користувачів, які отримують доступ до мережі або намагаються це зробити. Це дозволяє адміністраторам швидко виявляти та реагувати на будь-які підозрілі дії. Такі заходи допоможуть зменшити ризик витоку інформації та зберегти конфіденційні дані компанії в безпеці.

Розвиток сучасних технологій значно полегшив комунікацію та співпрацю між організаціями, проте сьогодні наявні нові виклики у сфері кібербезпеки. Зловмисники все частіше здійснюють атаки на менші компанії, з метою проникнення до цінних даних більших корпорацій.

Тому важливо, щоб будь-який договір або угода про співпрацю між підприємствами включала детальні вимоги щодо безпеки.

Шляхи та перспективи підвищення рівня інформаційної безпеки фірми, підприємства чи організації можуть залежати від її розміру. Більші підприємства зазвичай мають більші бюджети на інформаційну безпеку та можуть дозволити собі залучати більше кваліфікованих фахівців у цій галузі. Вони також можуть мати більше можливостей для використання новітніх технологій та інструментів для забезпечення безпеки даних. Однак, навіть невеликі підприємства можуть виявити високий рівень свідомості про інформаційну безпеку та розуміти важливість збереження даних. Вони можуть впроваджувати ефективні заходи з безпеки, такі як шифрування даних, заборону використання слабких паролів та резервне копіювання даних. Отже, розмір підприємства може впливати на

можливості для забезпечення інформаційної безпеки, але важливою є свідомість та підходи до захисту даних.

Задачі та механізми підвищення рівня інформаційної безпеки підприємства можуть залежати від його сфери діяльності. Наприклад, підприємства, які займаються обробкою та зберіганням конфіденційної інформації (наприклад, фінансові установи, медичні організації, державні установи), потребують більш високого рівня інформаційної безпеки порівняно з іншими підприємствами. З іншого боку, підприємства, які не займаються обробкою конфіденційної інформації, можуть потребувати менш жорстких заходів забезпечення інформаційної безпеки. У цьому відношенні варто зауважити, що сфера діяльності ТОВ «Глобал Вест» не належить до сфер, де захист інформації є критично важливим. Проте, незалежно від сфери діяльності, кожне підприємство має визнати важливість конфіденційної інформації та загалом інформаційної безпеки та приділяти достатню увагу її забезпеченню.

Зовнішні обставини можуть впливати на перспективи та методи підвищення рівня інформаційної безпеки підприємства. Наприклад, високий рівень загроз від кібератак може вимагати більш сильних заходів забезпечення безпеки, таких як кіберзахист або проведення комплексного аудиту безпеки інформації. Альтернативно, зміни в законодавстві або вимоги клієнтів можуть створювати нові вимоги до захисту конфіденційної інформації, що також може впливати на методи підвищення рівня інформаційної безпеки. В будь-якому випадку, підприємство повинно враховувати зовнішні обставини при плануванні та реалізації заходів забезпечення інформаційної безпеки.

Захист інформаційної безпеки може бути одним з ключових елементів стратегії розвитку фірми. У ТОВ «Глобал Вест» стратегія розвитку інформаційної безпек включає наступні елементи, пов'язані з захистом інформаційної безпеки:

1. Визначення пріоритетів інформаційної безпеки: Фірма може визначити ті області, де ризики безпеки найбільші, та спрямувати свої зусилля на захист цих областей.

2. Розробка політики безпеки: Фірма може розробити політику, що визначає правила та процедури, пов'язані з захистом інформації.

3. Підвищення обізнаності співробітників: Фірма може забезпечити навчання своїх співробітників з питань безпеки інформації, щоб зменшити ризик внутрішніх загроз.

4. Використання технологій захисту: Фірма може інвестувати у технології захисту, такі як антивірусне програмне забезпечення, брандмауери, системи контролю доступу та інші.

5. Аудит безпеки: Фірма може проводити регулярний аудит безпеки, щоб виявляти потенційні загрози та уразливості в системах та процедурах, пов’язаних з інформаційною безпекою.

6. Реагування на інциденти: Фірма може розробити плани реагування на інциденти, щоб зменшити можливі наслідки будь-яких порушень безпеки інформації.

Загалом, захист інформаційної безпеки повинен бути вбудованим у стратегію розвитку фірми та відображати реальні загрози, для забезпечення стійкості та успішності діяльності фірми, збереження довіри клієнтів та партнерів, конкурентної переваги, а також формування корпоративної культури.

У ТОВ «Глобал Вест» ефективність інформаційного забезпечення та підтримки у глобальній мережі наразі є низькою. Інформація, подана на сайті (див. вище рис.2.1) обмежена: присутні дані про контактну особу, керівника та головного бухгалтера, адреса, контактні (стаціонарні) телефони та кількість працівників. На сайті порожні розділи прайси, статті, новини, галерея, а у розділі «Продукція та послуги» присутні лише текстові дані «Виробництво і монтаж металопластикових вікон». Така ситуація негативно характеризує інформаційно-промоційну компанію й службу маркетингу підприємства, проте позитивно позначається на інформаційній безпеці ТОВ «Глобал Вест».

На сайті компанії слід вказувати обмежену кількість даних, щоб не зашкодити її інформаційній безпеці. Основні дані, які потрібно вказати, це контактні

дані компанії, такі як адреса, телефон та електронна пошта. Для більшої деталізації, можна вказати ім’я та посаду керівника компанії.

Непотрібно вказувати конфіденційну інформацію про компанію, таку як бухгалтерську звітність, договори з постачальниками та інформацію про клієнтів. Також не рекомендується вказувати детальну інформацію про працівників компанії, таку як їхній номер соціального забезпечення чи дату народження.

Для захисту від зловмисників, також важливо захистити сайт за допомогою відповідних заходів безпеки, таких як використання захищеного з'єднання HTTPS, регулярні оновлення програмного забезпечення та захист від зловмисного програмного забезпечення. Також важливо дотримуватися стандартів та законів щодо захисту персональних даних та конфіденційної інформації. Ці рекомендації слід обов’язково врахувати у майбутньому, коли підприємство буде більш активно використовувати ресурси глобальної мережі інтернет для пошуку клієнтів та співпраці із партнерами.

У організації доцільно використовувати різні канали комунікації в залежності від типу та конфіденційності передаваної інформації. Прикладами захищених каналів комунікації є: захищені електронні поштові сервіси з шифрування та автентифікацією; внутрішня корпоративна мережа; захищені месенджери, що використовують криптографічні протоколи для забезпечення безпеки інформації (дуже популярний сьогодні метод, практично усі користуються такими програмами, як Viber, Telegram, WhatsUp, Signal. Із цього переліку достатньо захищеним вважається останній, проте він найменш популярний); захищені хмарні сервіси (особливо коли йдеться про спільну роботу із електронними документами); захищені фізичні носії (використовують переважно лише для передачі даних з високим рівнем конфіденційності).

Таким чином, ми пропонуємо обмежити доступ усіх працівників до конфіденційної інформації та надання доступу лише до необхідних ресурсів. Побудова ієрархії доступів залежно від позиції та посади працівника дозволяє зменшити ризик несанкціонованого доступу до конфіденційної інформації.

Співробітництво з відділом безпеки (IT Security) є важливим етапом при вирішенні питань доступу до обмежених ресурсів. Вони можуть надати необхідний доступ користувачам за потреби, забезпечуючи контрольований та обмежений доступ до цих ресурсів. При цьому слід враховувати принцип найменшого можливого доступу, тобто надавати доступ лише до тих ресурсів, які дійсно потрібні для виконання роботи.

Крім того, важливо надавати навчання та інструкції співробітникам щодо захисту інформації та поведінки в мережі. Це може включати навчання про правила використання паролів, виявлення фішингових атак, безпечну обробку електронної пошти та інші аспекти інформаційної безпеки. Чим більше співробітники будуть обізнані та свідомі ризиків, тим ефективніше буде захист інформації підприємства.

Таким чином, враховуючи вразливість користувачів, впровадження ієрархії доступу та співпраця з відділом безпеки допоможуть забезпечити безпеку інформаційного середовища в ТОВ "Глобал Вест".

Висновки до другого розділу

В другому розділі проведено аналіз інформаційної безпеки ТОВ «Глобал Вест». Визначено чинники, які впливають на стан інформаційної безпеки: це людські чинники, технології, фізичне забезпечення і зовнішні загрози. Найбільшим у нашому випадку є вплив людського чинника, у його структурі можна виокремити ризики, пов’язані із

- діяльністю працівників підприємства,
- комунікації із партнерами та клієнтами,
- діяльністю третіх сторін, конкурентів та зловмисників

Механізми дотримання інформаційної безпеки у ТОВ «Глобал Вест» базуються на кількох засадничих позиціях: дотриманні політики безпечного поводження із конфіденційною інформацією; турботі про належний рівень обі-

знаності та інформаційної грамотності персоналу; належному технічному забезпеченні – використанні сучасних комп'ютерів із програмним забезпеченням, що вчасно оновлюється; моніторингу й аудиту інформаційних систем підприємства у тому числі з позицій інформаційної безпеки.

Перспективи підвищення рівня інформаційної безпеки ТОВ «Глобал Вест» пов'язані із строгим структуруванням службової інформації за рівнем доступу, використанням сучасного антивірусного програмного забезпечення, протидії методам соціальної інженерії шляхом належного навчання персоналу щодо поводження із особистими та корпоративними даними у соціальних мережах. Особливу увагу слід звернути на нерозголошення даних щодо поставок, контрактів, планів діяльності компанії, оскільки ТОВ «Глобал Вест» працює у секторі ринку із високою конкуренцією.

Для поліпшення рівня інформаційної захищеності компанії виокремлено такі пропозиції:

- визначитись із стратегією поводження із ризиками та дотримуватись її;
- більш активно розвивати мережеву присутність компанії із чітким розділенням рівнів доступу, оновити веб-ресурси компанії;
- проводити навчання персоналу щодо роботи із сучасним програмним забезпеченням на регулярній основі;
- використовувати захищені канали для комунікації у межах компанії.

ВИСНОВКИ

Обмін інформацією та інформаційна безпека відіграють ключову роль у діяльності підприємств та організацій. Важливість інформації серед іншого забезпечується тим, що інформація є основою для прийняття рішень, планування діяльності, вирішення проблем. Інформацію передають між суб'єктами обміну інформації за допомогою різних засобів через канали комунікації у вигляді текстових чи числових даних, аудіо й відео повідомлень, зображень, умовних сигналів тощо. Розрізняють технічний, семантичний та практичний аспекти при роботі з інформацією. У рамках технічного аспекту використовують математичні та ймовірнісні моделі для дослідження інформації, вимірювання її кількості та надійності передачі.

За ознаками збору, зберігання, перетворення, передачі інформації виділяють інформаційні системи. У складі технічних засобів автоматизованих інформаційних систем виокремлюють апаратну та програмну складову, кожна із яких може мати власні засоби для захисту інформації. Крім того, людський чинник відіграє дуже важливу роль у системі інформаційної безпеки, оскільки кінцевими реципієнтами інформації переважно є саме люди.

Інформаційна безпека передбачає захист важливої інформації від несанкціонованого доступу, пошкодження, втрати, розголошення тощо. Під важливою інформацією розуміють переважно конфіденційну інформацію, інформацію, що становить комерційну таємницю, інформацію, розголошення якої може завдати шкоди компанії, персональні дані працівників, клієнтів чи партнерів. У доступі до конфіденційної інформації можуть бути зацікавлені конкуренти чи зловмисники. Причинами порушення захисту інформації можуть бути людський чинник, недосконалість технічного забезпечення і системи захисту інформації, інші чинники.

Для захисту інформації від несанкціонованого доступу використовують розмежування доступу до документів за рівнем захисту, системи ідентифікації, аутентифікації та авторизації, методи шифрування даних при зберіганні та пе-

редачі, фізично захищені канали та сховища. Для захисту від втрат використовують надійні сховища та резервне копіювання. Для захисту цілісності даних використовують контрольні ключі та суми. Деякі сучасні програмні продукти містять вбудовані механізми захисту даних, наприклад, при втраті телефону або комп'ютера. Мережеві протоколи передачі даних також підтримують різні рівні захисту даних, що передаються.

Аналіз стану системи забезпечення інформаційної безпеки ТОВ «Глобал Вест» показує, що на підприємстві відсутній відділ, що займається системним захистом конфіденційної інформації. Сайт компанії містить деякі дані, які можуть бути використані для отримання сторонніми особами персональних даних про окремих працівників компанії, проте критично важливі для інформаційної безпеки даних у відкритому доступі немає.

Серед чинників, які найбільш помітно впливають на стан інформаційної безпеки підприємства є людський чинник, який пов'язаний із

- діяльністю працівників підприємства,
- комунікації із партнерами та клієнтами,
- діяльністю третіх сторін, конкурентів та зловмисників.

До інших чинників інформаційної безпеки ТОВ «Глобал Вест» можна зарахувати технологічний чинник, процеси і процедури обміну інформацією на підприємстві, технічне забезпечення автоматизованої інформаційної підсистеми підприємства та потенційні зовнішні загрози.

Механізми гарантування інформаційної безпеки у ТОВ «Глобал Вест» використовують такі суттєві елементи, як дотримання політики безпечного поводження із конфіденційною інформацією, сприяння належному рівню вмінь та навичок персоналу по роботі із даними й дотриманні інформаційної гігієни; сучасному технологічному обладнанні, підтримці антивірусних й антишпигунських програм у актуальному стані, регулярному проведенні моніторингу й аудиту інформаційних систем підприємства.

Напрями та перспективи підвищення рівня інформаційної безпеки ТОВ «Глобал Вест» передбачають системний аналіз ризиків порушення інформа-

ційної безпеки, належне дотримання правил роботи із інформацією для службового використання та із обмеженим доступом, використанням технічних засобів як от антивірусів та мережевих екранів, організації комунікації через захищені канали, протидії застосуванню методів соціальної інженерії для розкриття даних про працівників та клієнтів, а також важливої ділової та фінансової інформації шляхом належного навчання персоналу щодо поводження із особистими та корпоративними даними у соціальних мережах. Особливу увагу слід звернути на нерозголошення даних щодо поставок, контрактів, планів діяльності компанії, оскільки ТОВ «Глобал Вест» працює у секторі ринку із високою конкуренцією.

Для поліпшення рівня інформаційної захищеності компанії можна рекомендувати дотримуватись стратегії оцінки та мінімізації ризиків, оновити вебресурси компанії, проводити навчання та тренування персоналу щодо роботи із сучасним програмним забезпеченням, регулярно виконувати заході із тестування інформаційної безпеки компанії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авраменко А.С., Авраменко В.С., Косенюк Г.В. Тестування програмного забезпечення: навчальний посібник. Черкаси: ЧНУ імені Богдана Хмельницького, 2017. 284 с.
2. Адамська І. Сучасний стан й тенденції розвитку будівельної галузі України. *Галицький економічний вісник*. 2019. № 5. С. 7-15.
3. Блага Н., Приймак І. Наслідки впливу глобалізації на політику державного регулювання фінансового ринку. Nowoczesna edukacja: filizofia, innowacja, doswiadczenie. Lodz Wysza Szkola Informatyki i Umiejetnosci. 2015. № 4. С.200-206.
4. Блага Н., Приймак І. Побудова моделей вибору стратегії розвитку підприємства в умовах конкуренції.
   URL: http://dx.doi.org/10.30970/meu.2019.41. 0.2822
5. Блага Н.В., Приймак І.І. Соціальні аспекти системи оподаткування доходів фізичних осіб в Україні. *Соціально-правові студії: науково-аналітичний журнал*. Львів: ЛьвДУВС. 2018. Вип. 1. С. 72-80.
6. Бобик О. В. Теорія ймовірностей і математична статистика: підручник. Київ: ВД «Професіонал», 2007. 560 с.
7. Виробництво вікон в Україні скоротилося втричі проти 2021р. Інтерфакс-Україна. URL: https://interfax.com.ua/news/economic/852327.html
8. Глинський Я.М. Практикум з інформатики. Львів, 2001. 224 с.
9. Глобал Вест, ТОВ Бізнес-Гід. URL: https://global-west. business-guide.com.ua/
10. Головне управління статистики у Львівській області. URL: https://www.lv.ukrstat.gov.ua/
11. Грищенко В.О. Теорія ймовірностей та математична статистика для економістів: навчальний посібник. Київ: КДТЕУ, 2000. 170с.

12. Живко З. Б. Механізм управління системою економічної безпеки підприємства. *Науковий вісник Ужгородського університету*. 2014. Вип. 3. С. 37-42. URL: http://nbuv.gov.ua/UJRN/ Nvuuec_2014_3_11
13. Жураковський Ю.П., Полторак В.П. Теорія інформації та кодування: підручник. Київ: Вища школа, 2001. 255с.
14. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*. 2010. № 3. С. 123-129.
15. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР
URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
16. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI
URL: https://zakon.rada.gov.ua/laws/main/2297-17#Text
17. Кузьмін І.В. Основи теорії інформації та кодування: підручник. Хмельницький : ХНУ, 2009. 373 с.
18. Кулик А.Я., Кривогубченко С.Г., Теорія інформації і кодування. навч. посібник. Вінниця: ВНТУ, 2008. 145 с.
19. Курко А.М. Введення в теорію інформації: посібник. Тернопіль. 2017 108с. URL: http://elartu.tntu.edu.ua /handle/lib/21919
20. Нехай В. А. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент*. 2017. Вип. 24(2). С. 137-140. URL: http://nbuv.gov.ua/UJRN/Nvmg u_eim_2017_24%282%29__30
21. Офіційний сайт Державної служби статистики України.URL: www.ukrstat.gov.ua
22. Про компанію Open Teck : URL: https://www.openteck.com.ua/ua/
23. Сакун О.С., Щур Р.І, Мацьків В.В. Фінансові аспекти підтримки бізнес-сектору України в умовах воєнного стану. *The actual problems of regional economy development*. 2002. 1(18), 50-60.

24. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки*, 2016. (1), 155-161.
25. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету*, 2010. 2(2), 32-35.
26. ТОВ «ГЛОБАЛ ВЕСТ» : URL: https://opendatabot.ua/c/33252468
27. Тулякова Н. О. Теорія інформації: навчальний посібник. Суми: Вид-во СумДУ, 2008. 212 с.
28. Череп А.В. Формування стратегії інвестиційної діяльності підприємства. Економічний вісник університету. 2011, № 2 (19) С. 12-15.
29. Чешук В.О. Діагностування рівня розвитку будівництва в Україні. Вісник Черкаського університету. 2018. № 2. С. 87–95
30. Ширяєва Н.В., Макаренко А.Б. Дослідження впливу пандемії COVID-19 на економіку України як одного із факторів глобальної фінансової кризи. *Вісник НТУ "ХПІ"*. 2020. №4. С. 86–94.
31. Hakemi A., Jeong S. R., Ghani I., Sanaei M. G.. Enhancement of VECTOR method by adapting OCTAVE for risk analysis in legacy system migration. *KSII Transactions on Internet and Information Systems* (TIIS), 2014. 8(6), 2118-2138.
32. Hashim N. A., Abidin Z. Z., Puvanasvaran A. P., Zakaria N. A., Ahmad R. (2018). Risk assessment method for insider threats in cyber security: A review. *International Journal of Advanced Computer Science and Applications*, 9(11).
33. Ziobrowski P. Bezpieczeństwo informacji we współczesnej firmie. *Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa*, 2009. (1), 77-84.