МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНТРІШНІХ СПРАВ
ЦЕНТРУ ПІСЛЯДИПЛОМНОЇ ОСВІТИ, ЗАОЧНОГО
ТА ДИСТАНЦІЙНОГО НАВЧАННЯ

Кафедра менеджменту

Кваліфікаційна робота

на тему:

ІНФОРМАЦІЙНА БЕЗПЕКА ПРОВЕДЕННЯ ІНВЕСТИЦІЙНОЇ ПОЛІТИКИ НА ПІДПРИЄМСТВІ

Здобувача вищої освіти освітнього
ступеня «магістр»
2 курсу заочної форми навчання
Спеціальності 073 «Менеджмент»
Тетяни Володимирівни
ПОНОМАРЬОВОЇ

Науковий керівник:
кандидат економічних наук, доцент
Наталія Василівна БЛАГА

Рецензент
кандидат економічних наук, доцент
Ірина Ігорівна ПРИЙМАК

Кваліфікаційна робота допущена до захисту
«____» **_____**2022р., протокол №__

Завідувач кафедри менеджменту
_____

Львів – 2022

АНОТАЦІЯ

Пономарьова Т.М. Інформаційна безпека проведення інвестиційної політики на підприємстві. – Рукопис.

Дослідження на здобуття освітнього ступеня магістр за спеціальністю 073 «Менеджмент». – Львів, 2022.

Досліджено теоретичні основи інформаційної безпеки проведення інвестиційної політики на ТОВ «Глобал Вест». Визначено особливості проведення інвестиційної політики на підприємстві.

Обсяг роботи становить 50 сторінок, включаючи 11 рисунків.

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

Ключові слова: інформаційна безпека, інвестиційна політика, комунікаційний процес.

ANNOTATION

Ponomareva T.M. Information security of investment policy at the enterprise. - Manuscript.

Research for a master's degree in 073 "Management". - Lviv, 2022.

The theoretical foundations of information security of investment policy at Global West LLC have been studied. The peculiarities of investment policy at the enterprise are determined.

The volume of the work is 50 pages, including 11 figures.

On the basis of elaboration of materials of theoretical and practical character the corresponding conclusions are made and concrete offers are brought.

Key words: information security, investment policy, communication process.

ЗМІСТ

ВСТУП

Розвиток ринкових відносин в Україні визначає діяльність організації та умови її функціонування. Щоб організації вижили, вони повинні правильно визначити свою ринкову стратегію та тактику. А також систематично керувати робочою силою, щоб вона приносила прибуток.

Поняття загроз інформаційній безпеці зародилося майже одночасно з інформаційним середовищем. Спочатку він мав ознаки крадіжки комп'ютерної інформації, шахрайського та незаконного використання, а також пошкодження комп'ютерної інформації. Пізніше, з розвитком інформаційних систем, інформаційна загроза стала засобом проникнення у вірусні мережі. Сьогодні безпека впливає майже на всіх у глобальному інформаційному середовищі. В Україні це робиться на національному рівні та в межах кожної окремої компанії.

Нині в Україні діє близько трьох тисяч законів, які регулюють, захищають та підтримують інформаційні відносини з громадськістю. Законодавство України у сфері інформації та інформаційної безпеки базується на: Конституції України, ряді кодексів, законі про інформацію, законі про захист інформації в автоматизованих системах та багатьох інших спеціальних законах.

Керівництво вимагає від керівників спілкування зі співробітниками, щоб мотивувати їх ефективно виконувати завдання. Організаційна діяльність керівника вимагає збору інформації про ситуацію на підприємстві, яка роз'яснює працівникам принципи, методи та цілі роботи.

Спілкування сьогодні стає все більш важливим і цінним. Особливу увагу варто звернути саме на безпеку інформаційного процесу в організації. Адже підприємець може зазнати величезних збитків через нехтування інформаційними носіями або втратити навіть компанію в цілому. Тому тема важлива і потребує глибокого дослідження.

Немало вчених досліджували питання безпеки інформації на підприємстві, а саме це М.Крупка, О.Крюков, В.Цимбалюк [2-5] та інші. Проте донині ці питання залишаються актуальними і потребують детального вивчення.

Метою даної роботи є вивчити механізм інфомаційної безпеки в системі інвестиційної політики підприємства.

Для досягнення поставленої мети необхідно вирішення таких завдань:

розглянути сутність операційного процесу підприємства;

– визначити сутніть інформаційної безпеки на підприємстві та необхідність;

– розглянути основні типи інтернет-загроз в системі інвестиційної політики підприємства;

– проаналізувати господарську діяльність та систему інформаційної безпеки інвестиційної політики ТОВ «Глобал Вест»;

– надати пропозиції та напрямки вдосконалення інформаційної безпеки на ТОВ «Глобал Вест».

Об'єктом дослідження є безпека інформаційного процесу та його інвестиційної політики на підприємстві.

Предметом дослідження є інвестиційна політика на ТОВ «Глобал Вест» та його інформаційна безпека.

Методи дослідження. Теоретичною базою кваліфікаційної роботи є наукові дослідження вітчизняних та зарубіжних вчених з питань стратегічного менеджменту підприємства. Для досягнення поставленої мети в роботі використано такі загальнонаукові та спеціальні методи: системного аналізу та синтезу, статистичний метод, моделювання та інтегральної оцінки, експертних оцінок, а також метод узагальнення результатів.

Інформаційною базою кваліфікаційної роботи є наукові доробки вітчизняних та зарубіжних вчених, матеріали науково-практичних конференцій та інтернет видань, а також результати власних досліджень.

Апробація результатів. Теоретичні положення та практичні пропозиції обговорювалися на VIII Всеукраїнській студентській науково-практичній конференції «Сучасний менеджмент: витоки, реалії та перспективи розвитку», яка відбулася 10 березня 2022 р.

Структура роботи. Робота містить три розділи, вступ, висновки та пропозиції, список використаних джерел.

На основі опрацювання теоретичних та практичних матеріалів розроблені відповідні висновки та обґрунтовано конкретні пропозиції.

Зміст кваліфікаційної роботи викладено на 50 сторінках.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ІНВЕСТИЦІЙНОЇ ПОЛІТИКИ НА ПІДПРИЄМСТВІ

1.1 Сутність комунікаційного процесу та інформаційної безпеки підприємства

Нестабільна і в багатьох випадках деструктивна економічна ситуація, в якій зараз перебуває вся Україна, а відповідно і більшість компаній, досить чітко відображає проблему інформаційної безпеки в державі і в компанії зокрема. Тому що ефективна інформаційна безпека на практиці є необхідною умовою для досягнення цілей компанії. Відсутність прозорості, часто через недосконалу систему комунікацій, значно знижує ефективність управління та функціонування компанії.

Комунікація є важливим елементом прибуткової компанії. У сучасних компаніях комунікація вже давно перестала бути лише засобом передачі інформації і стала одним із важливих інструментів управління діловими відносинами. Інформація, комунікація разом із засобами, що забезпечують їх ефективне використання, тобто канали, формують інфраструктуру управління компанією.

Комунікаційний процес — це процес передачі інформації від однієї людини до іншої або між групами людей за допомогою різних каналів і різних засобів комунікації (вербальні, невербальні тощо).

Для того, щоб керівник ефективно виконував свої завдання, він повинен планувати роботу контрольного об’єкта, організовувати її, розподіляти завдання між безпосередніми постачальниками та забезпечувати їх необхідними ресурсами, залучати працівників до дорученої роботи, контролювати результати та коригувати їх. якщо необхідно. діяльності. Цю роботу неможливо виконати без чіткого уявлення про стан будівлі, яким вона керує, та її оточення, що

можливо лише за наявності відповідної інформації. Тому вони становлять основу процесу управління інформацією. Робота менеджера на 50-70% складається з інформаційної роботи. Сюди входять обробка документів, заплановані та позапланові зустрічі, телефонні дзвінки, відвідування нарад і зустрічей тощо. Спілкування – це процес передачі інформації від однієї людини до іншої [5].

Велике значення мають комунікаційні технології. Адже використання правильних висловів, точних виразів, зображувальних матеріалів, технічних засобів тощо, інтонація голосу, через допоміжні слова, що використовуються при обміні інформацією вагомим чином впливають на співрозмовника. Щоб передати повідомлення, слова потрібно правильно поєднувати з невербальними засобами.

Тому для ефективної та ефективної комунікації, надання інформації у відповідній формі, необхідно враховувати ряд факторів, а саме правильний вибір слів при створенні звіту, потреби адресатів, прозорість звіту, правові вимоги [1].

На початку 1960-х років лише в зарубіжній філософсько-соціологічній літературі було близько сотні визначень передачі інформації, але сьогодні можна з упевненістю сказати, що їх набагато більше. Існує цілий ряд перспектив, аспектів, розділів, спроб загальнотеоретичного та конкретного підходу до дослідження та розуміння комунікації.

Одним із важливих чинників інтеграції лідерства є спілкування, тобто спілкування людей у процесі їх спільної дії: обмін думками, ідеями, почуттями та інформацією. Жодна організована група людей не може існувати без спілкування.

Тому ефективна міжособистісна комунікація є важливою для успіху організації. Він характеризується такими факторами:

– вирішення багатьох управлінських завдань ґрунтується на безпосередній взаємодії людей (начальника з підлеглим, підлеглих з іншим підлеглим) між різними подіями;

− міжособистісне спілкування є, мабуть, найкращим способом обговорення та вирішення проблем, що характеризуються невизначеністю та двозначністю.

Таким чином, керівник повинен усвідомлювати, що інформаційна безпека є надзвичайно важливою не лише для підприємства, ай для кожного працівника зокрема. Відповідно і процес комунікації в організації вимагає особливої уваги.

Спілкування може відбуватися різними способами - письмово, усно, з використанням невербальних сигналів (жести, міміка тощо) і через різні канали – віч-на-віч, по телефону, на конференції, за допомогою електронного чи електронного спілкування. . Кожен із методів і каналів має переваги та недоліки, залежно від їх використання.

Методи спілкування можна комбінувати один з одним, щоб бути більш ефективними. Крім одночасного використання елементів вербальної та невербальної комунікації, можна вказати на більш широке поєднання усного спілкування з паралельними інструкціями, створеними за допомогою графіків, таблиць, графіків та інших фіксованих зображень, які є конфігурацією письмової інформації. Це значно спрощує сприйняття, особливо якщо розуміння складне і займає багато часу.

При виборі способу комунікації необхідно враховувати певні обставини, пов’язані з процесом обміну інформацією. Тому усне спілкування слід використовувати, коли інформацію потрібно надати негайно, а зворотній зв’язок негайно підтверджує правильне розуміння надісланої інформації. Невербальні сигнали, які найчастіше супроводжують вербальне спілкування, допомагають правильно зрозуміти інформацію, і тому їх слід враховувати. Письмове спілкування є більш прийнятним, ніж усне з точки зору важливих деталей і коли клієнтам потрібно зберігати дані. У деяких випадках усне та письмове спілкування потрібно поєднувати (ми можемо домовитися про це по телефону, а потім надіслати письмово, щоб адресат запам’ятав).

Інформаційну безпеку компанії досліджували багато вчених, зокрема В. Цимбалюк стверджує, що інформаційна безпека підтримує правильний

(необхідний, можливий) рівень життя інформаційної системи, у тому числі бізнесоності [2]. О. Сороківська вважає, що концепція інформаційної безпеки на підприємстві – це суспільні відносини щодо створення та підтримки на належному рівні інформаційної системи суб'єкта господарювання [3].

О. Крюков обґрунтовує «інформаційну безпеку» як суспільно законодавчі відносини згідно процедури організації створеня, обслуговування, захисту та оборони, необхідної для особи (фізична або юридична особа, установа, підприємство, організація), компанія та безпечні умови життя; зв'язки з громадськістю пов'язані з організацією технологій створення, розповсюдження, зберігання та використання інформація (інформація, дані, знання) для забезпечення функціонування та розвитку інформаційні ресурси людей, суспільства та країни [4].

Безпека бізнесу – це стан сталого життя, що забезпечує реалізацію основних інтересів і пріоритетів компанії, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування. Беручи до уваги визначення поняття «безпека бізнесу», можна зробити висновок, що головною метою безпеки бізнесу є нейтралізація та усунення загроз належному веденню бізнесу в Україні, що призводять до будь-якої форми втрати активів чи прибутку. може призвести до бізнесу [10].

Однією з форм безпеки бізнесу є інформаційна безпека компанії. Як зазначається у статті, у сучасній науці досі недостатньо уваги до проблеми визначення поняття «безпека ділової інформації», про що свідчать слабкі концептуальні дослідження. Найпоширеніші визначення поняття «безпека бізнес-інформаційної безпеки» включають:

− зв'язки з громадськістю для створення та підтримки відповідної інформаційної системи, включаючи операції на належному (необхідному, можливому) рівні життя;

− зв'язки з громадськістю, метою яких є створення та підтримка інформаційної системи економічного оператора на належному рівні життя [3];

– співвідношення між рівнем захисту інформації та рівнем інформаційної загрози; комплекс засобів і заходів уповноважених осіб, спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури підприємства в процесі обміну, обробки та зберігання інформації на всіх рівнях ІТ-системи підприємства.

Основні компоненти інформаційної безпеки України (рис.1.1).

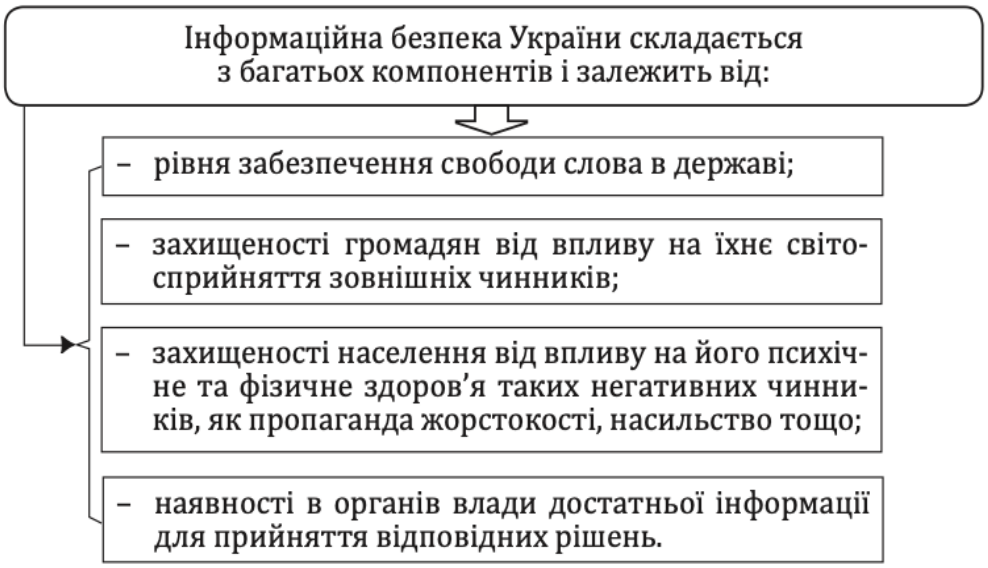


Рис.1.1 Компоненти інформаційної безпеки України [10]

Отже, забезпечення інформаційної безпеки бізнесу в Україні є комплексним завданням, яке вимагає від органів державної влади вжиття низки адміністративно-правових та організаційних заходів, спрямованих на забезпечення ефективності системи інформаційної безпеки суб'єктів господарювання, у тому числі розробку стратегії державного бізнесу. інформаційної безпеки, розробка заходів з організації навчання персоналу суб'єктів господарювання основним принципам інформаційної безпеки, визначення відповідальності за порушення принципів захисту інформації.

Ми вважаємо, що інформаційна безпека підприємства – це система безпеки інформації підприємства та захисту від злодійства, невчасного і неточного подання її одержувачу.

1.2 Основні заходи забезпечення інформаційної безпеки інвестиційної політики на підприємстві

Чимало підприємств, особливо із тих, що мають справу із клієнтами – фізичними особами, починаючи із 2010 року повинні слідкувати за дотримання закону, що стосується захисту персональних даних. В Україні зазвичай дотримання цього закону зводиться до того, що клієнтам банків, підприємств, фірм та корпорацій доводиться підписувати додаткові папери або ставити відмітку у додатковому пункті стандартної угоди, зміст якої стосується так званого захисту їх персональних даних. Робота з персональними даними, у тому числі дотримання правил їх нерозголошення й нерозповсюдження та коректного використання є однією із важливих компонент інформаційної безпеки підприємства. Слід зазначити, що згадані вимоги у законодавство України запозичено із світової практики. Більш детально особливості роботи підприємств у тому, що стосуються захисту персональних даних, розкрито у книзі [22] та інших.

Для фахівців із інформаційної безпеки найбільш розумним методом забезпечення відповідності законодавчим вимогам є забезпечення найвищого рівня контролю безпеки всім даним, пов’язаним з окремими клієнтами чи співробітниками. Щоб забезпечити такий контроль, має статися перше і найважливіше завдання управління ризиками: класифікація даних.

Інформація, пов’язана з конфіденційністю — елементи даних, які окремо або в поєднанні з іншими даними належать до окремої особи — повинна бути віднесена до найбезпечнішої категорії. Організації часто позначають цю категорію як «цілком секретна», «персональна інформація», «з обмеженим доступом», «конфіденційна», «конфіденційна» або подібним описовим ярликом. Багато спеціалістів з дотримання вимог вважають за краще, щоб класифікації були зрозумілими; таким чином, терміни «непублічна особиста інформація» або «персональна інформація» можуть бути кращими як тип класифікації, яка описує дані, пов’язані з конфіденційністю. Вибране конкретне ім’я є менш важливим,

ніж встановлення категорії, яка явно включає дані, пов'язані з окремими особами. Так, для осіб, що мали справу із документацією обмеженого доступу ще за часів Союзу, звичним є шифр ДСК (для службового користування), а тому такі міри обмеження доступу і у нас мають давню історію, хоча раніше користувались вузьких областей і більшість населення за усе життя так і не стикались із допусками тощо. Крім того, необхідно розробити та опублікувати письмову політику, що пояснює різні види даних, що входять до класифікації, та супроводжується легко сприйнятливими прикладами для внутрішнього організаційного використання. Інформаційна безпека буде сприяти формуванню цієї політики, хоча автором фактичного документа може бути юридичний відділ, відповідність або подібна функція контролю. Політика має бути доступною для всіх працівників.

Завдання ідентифікації даних, пов'язаних з конфіденційністю, що також включає документування електронного розташування цих даних і методів, за допомогою яких дані передаються всередині організації та зовнішнім організаціям, найкраще виконують зацікавлені сторони бізнесу та технологи, які підтримують системи та програми, що використовуються зацікавленими сторонами. Проте, інформаційна безпека, яка виконує обов'язкові правила конфіденційності, не є лише пасивним спостерігачем за процесами ідентифікації та класифікації. Фактично, персонал із інформаційної безпеки повинен гарантувати, що класифікація відбувається таким чином, щоб технічні засоби контролю безпеки (наприклад, шифрування, дизайн безпечної архітектури, механізми контролю доступу) належним чином виконували свої призначені функції [12].

Розвиток інформаційних технологій і засобів комунікації створює все більше можливостей для доступу до інформаційних ресурсів і необмеженого переміщення великих масивів даних. У той же час доступ широкого кола користувачів, який може бути довільним, до ресурсів, розташованих у будь-якій точці глобальної інформаційної мережі, збільшує загрозу інформаційним ресурсам компанії та інформаційній системі компанії в цілому. Тому така

інформація, як продукт, який ви шукаєте, потребує збереження та надійного захисту.

Одним із найважливіших заходів забезпечення інформаційної безпеки компанії є виявлення, оцінка та запобігання загрозам інформаційної безпки та інформаційним ресурсам. Сучасна система інформаційної безпеки компанії призначена для захисту конфіденційної інформації від несанкціонованого доступу, запобігання зловмисним або випадковим змінам (перевірки цілісності) та забезпечення необхідного рівня доступу. Забезпечення інформаційної безпеки обмежується трьома основними напрямками – поєднанням технічних, адміністративних та організаційних заходів.

Таким чином, у сучасній бізнес-ситуації, коли інформаційна безпека набуває глобального характеру, вона є невід'ємною частиною системи економічної безпеки суб'єкта господарювання та економічної безпеки країни в цілому.

Отже, інформаційна безпека процесу інвестиційної політики є системою захисту корпоративної інформації; захист від крадіжки, передчасне і неточне пред'явлення одержувача. Нехтуючи інформаційними носіями, підприємець може зазнати значних збитків або взагалі втратити свою компанію.

Висновки до першого розділу

В першому розділі нами досліджено теоретичні основи інформаційної безпеки в системі інноваційної політики підприємства. Виокремлено сутність інформаційної безпеки підприємства. Таким чином, інформаційна безпека компанії – це система інформаційної безпеки компанії та захисту від крадіжки, несвоєчасного та недостовірного подання одержувачу.

Визначено основні заходи забезпечення інформаційної безпеки на підприємстві та дано їм короткі характеристики.

Таким чином, одним з найважливіших заходів забезпечення інформаційної безпеки компанії є виявлення, оцінка та запобігання загроз інформаційній безпеці та інформаційним активам. Сучасна система інформаційної безпеки компанії призначена для захисту конфіденційної інформації від несанкціонованого доступу, запобігання зловмисним або випадковим змінам (перевірки цілісності), забезпечення необхідного рівня доступу. Забезпечення інформаційної безпеки обмежується трьома основними напрямками – поєднанням технічних, адміністративних та організаційних заходів.

РОЗДІЛ 2.
АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ПРОВЕДЕННЯ ІНВЕСТИЦІЙНОЇ ПОЛІТИКИ ТОВ «ГЛОБАЛ ВЕСТ»

2.1 Загальна характеристика підприємства ТОВ «Глобал Вест»

Товариство з обмеженою відповідальністю «Глобал Вест».

Основним видом діяльності ТОВ «Глобал Вест» є неспеціалізована оптова торгівля, її різновиди представлені на рисунку 2.1.

За свою 18-річну історію компанія займалася різними видами діяльності, але останнім часом все більше спеціалізується на виробництві пластикових профілів для віконних та дверних систем під брендом Open Teck. Open Teck вже 7 років - найбільший український виробник ПВХ від 100 до 700 мм на 50 мм, а також пластикових стоків і комплектуючих.

Статутний капітал ТОВ «Глобал Вест» становить 23 700 грн.

- Діяльність посередників у торгівлі товарами широкого асортименту
- Оптова торгівля деревиною, будівельними матеріалами та санітарно-технічним обладнаням
- Складське господарство
- Механічне оброблення металевих виробів
- Виробництво інших виробів із пластмас
- Виробництво будівельних виробів із пластмас
- Виробництво труб, листів, профілів із пластмас

Рис.2.1 Види діяльності ТОВ «Глобал Вест»

Спочатку компанія почала розповсюджувати один тип вікон покупцям у Львівській області, але досить швидко (за кілька місяців) освоїли інші типи, що призвело до розширення асортименту продукції. Завдяки злагодженій роботі з командою Open Teck та додатковим інвестиціям у виробничі потужності, компанія зайняла лідируючі позиції в рейтингу компаній, що займаються монтажем та доставкою віконних систем в області та навіть за межі області. Open Teck є основним виробником і постачальником віконних систем та комплектуючих до них для компанії ТОВ «Глобал Вест».

Здійснюючи вищезазначені заходи, організація досягає своїх цілей.

Проте в останні три роки чистий прибуток був від'ємним (рис.2.2). Можна констатувати, що фінансова діяльність ТОВ «Глобал Вест» збиткова.

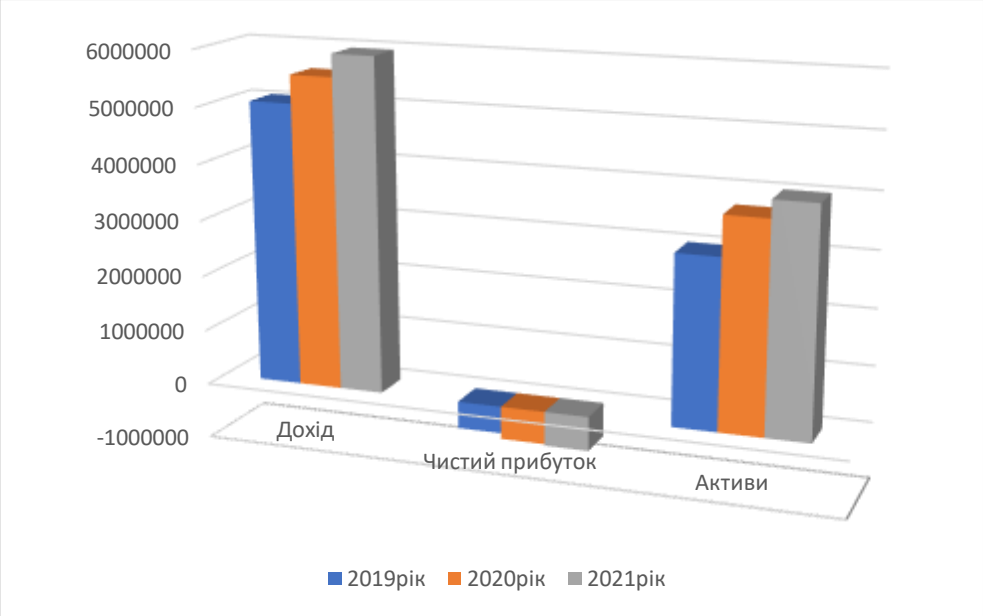


Рис. 2.2. Динаміка показників фінансової ділності ТОВ «Глобал Вест», 2019-2021рр

З проведених досліджень, бачимо що чистий прибуток спадає, найвищий його результат у 2019 році і становить 6233550грн. Це пояснюється зменшенням попиту за відповідним напрямком діяльності. Чистий прибуток є найменшим порівняно з іншими показниками, проте за останніх три роки він не набув вагомих змін (рис. 2.3).

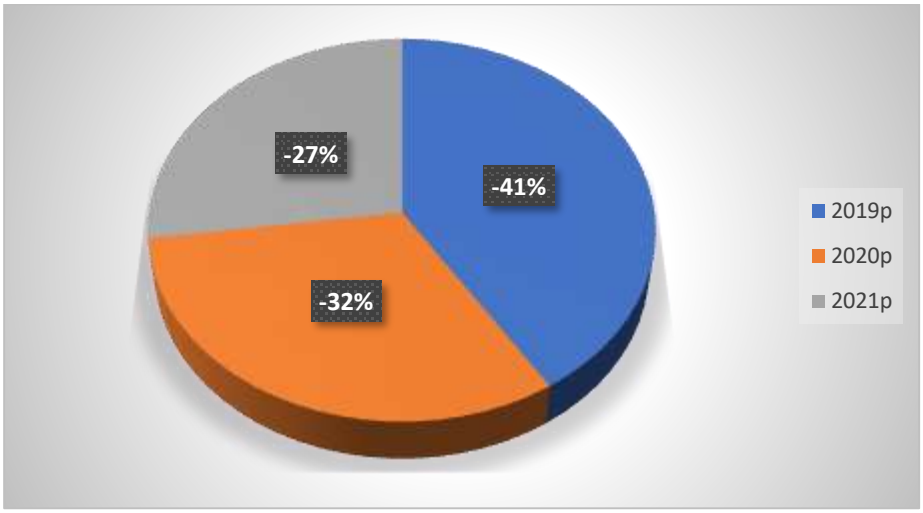
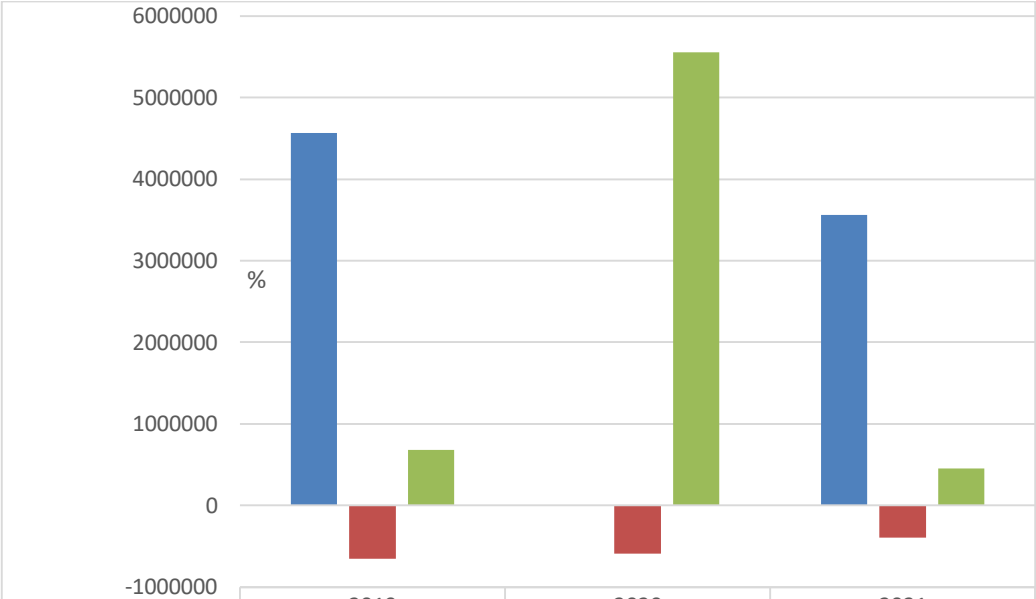


Рис.2.3 Динаміка чистого прибутку ТОВ «Глобал Вест» за 2019-2021р

Згідно з проведеним аналізом, можна констатувати, що досліджуване товариство ефективно працювало до 2019 року. Далі доходи та чистий прибуток продовжували знижуватися.

Товариство з обмеженою відповідальністю здійснює свою діяльність у законодавчій сфері України відповідно до Господарського кодексу України. Господарська діяльність ведеться на підставі статуту. Відносини регулюються Конституцією України, Господарським кодексом, законами України, постановами Президента України та Кабінету Міністрів України, розпорядженнями інших органів державної влади та місцевого самоврядування та іншими нормативно-правовими актами. Діяльність також регулюється на підставі рішень Загальних зборів акціонерів, Спостережної ради, Правління (голови Ради директорів) та Ревізійної комісії.

З метою визначення фінансового стану ТОВ «Глобал Вест» необхідно проаналізувати основні фінансові показники та результати діяльності підприємства. Оскільки відомо, що у мінливих зовнішніх умовах конкурентною перевагою виступає саме фінансова стійкість субєкта господарювання, що виступає гарантом його надійності та довговічності.



	2019	2020	2021
Активи	4568745	0	3561000
Чистий прибуток	-653981	-586500	-393291
Дохід	678327	5557700	455820

Рис.2.4 Динаміка зміни відносних показників господарської діяльності ТОВ «Глобал Вест»

Сутність фінансової діяльності підприємства полягає у забезпеченні систематичного надходження фінансових ресурсів та їх ефективного використання, дотримання принципів та вимог ведення розрахунків, кредитних зобов'язань, досягнення раціональності у співвідношенні власного та залученого капіталу, забезпечення фінансової стійкості підприємства, як одного із ключових елементів його економічної безпеки.

Керівництво ТОВ «Глобал Вест» чітко розуміє, що інформаційна безпека підприємства є основоположною для життя організації та сприяє реалізації, контролю та дотриманню вимог прийнятої Політики.

У ТОВ «Глобал Вест» створено та постійно створюється колективний орган – Комісія системи управління інформаційною безпекою Товариства з обмеженою відповідальністю «Глобал Вест», рішення якого є обов'язковими для виконання всіма працівниками товариства.

Документи, пов'язані з системою інформаційної безпеки управління підприємством, готуються структурними підрозділами за відповідними

напрямками діяльності та є доступними для працівників підприємства у сфері їх компетенції та покликані допомогти задовольнити вимоги інформаційної безпеки.

Комісія з інформаційної безпеки підприємста несе відповідальність за моніторинг впровадження, впровадження та вдосконалення політики.

На даний момент функціонування Політики інформаційної безпеки покладено на начальника відділу інформаційної безпеки.

Кожен працівник ТОВ «Глобал Вест» забезпечує підтримання належного рівня інформаційної безпеки підприємства в межах своїх обов'язків та посадових прав і несе відповідальність за їх порушення відповідно до законодавства України та внутрішніх нормативних актів.

Система інформаційної безпеки проведення інвестиційної політики на ТОВ «Глобал Вест» переглядається за необхідності, але не рідше одного разу на рік. Причинами внесення змін до є зміни правових, нормативних та інших стандартів.

2.2 Дослідження інформаційної безпеки проведення інвестиційної політики на ТОВ «Глобал Вест»

Політика інформаційної безпеки проведення інвестиційної політики у Товаристві з обмеженою відповідальністю «Глобал Вест» описує та регулює роботу системи управління безпекою інформації відповідно до національних стандартів інформаційної безпеки в Україні.

Складність і масштаби інформаційних загроз з кожним роком збільшуються.

Також експерти поділяють загрози на внутрішні та зовнішні, форс-мажорні та штучні. До форс-мажору належать усі фактори, пов'язані зі стихійним лихом або нездоланними перешкодами: пожежа, землетрус, війна ураган тощо.

Теорія і практика вказують на існування двох груп загроз інформаційній безпеці суспільства, таких як ненавмисні або випадкові дії, що призводять до недостатнього забезпечення безпеки та помилок управління, та навмисних загроз – несанкціонований доступ до інформації та несанкціоноване маніпулювання даними. . ресурси та самі системи.

Класифікацію загроз інформаційної безпеки також можна поділити на загрози, пов’язані з внутрішніми та зовнішніми факторами.

Дії конкретної особи є штучними: хакерська атака, помилка або навмисні дії офіційного користувача, що призвели до надзвичайної ситуації.

Слід підкреслити ризик навмисних помилок поза суспільством. Такі загрози включають [11; 3]:

− несанкціонований доступ до інформації, що зберігається в системі;

− відмова від кроків, пов'язаних з маніпулюванням інформацією (наприклад, несанкціоноване внесення змін, що призводить до порушення цілісності даних);

− впровадження «логічних бомб» у програмне забезпечення та проекти, які виконуються за певних умов або через певний час і частково чи повністю вимикають комп’ютерну систему;

− розробка та поширення комп'ютерних вірусів;

− недбалість у розробці, обслуговуванні та експлуатації програмного забезпечення, що призводить до краху комп'ютерної системи;

− зміна комп'ютерної інформації та фальсифікація електронних підписів;

− крадіжка інформації з подальшим маскуванням;

− фіксування інформаційних потоків;

− відмова від здійснення діяльності чи надання послуг;

− відмова від надання послуги.

Зауважимо, що єдиного підходу до класифікації загроз інформаційній безпеці не існує, оскільки при всьому різноманітті інформаційних систем, призначених для автоматизації багатьох технологічних процесів, що впливають на різні сфери людської діяльності, жорстка систематизація та класифікація

загроз є неприпустимим. Після огляду джерел можна запропонувати наступну класифікацію небезпеки:

Виникнення та наслідки - кримінальне правопорушення; шахрайство; хуліганство.

- За типом – програмне забезпечення; обладнання, інше.
- Мета оперативна, тактична, стратегічна.
- Залежно від характеру подій – навмисні, ненавмисні.
- За ІТ – предмет загроз, методи підготовки загроз, інструменти загроз, середовище загроз.
- За місцем походження – всередині, зовні.
- Залежно від суб’єкта впливу – системні, локальні.
- У зв'язку з виникненням неполадків в системі, а саме збій апаратного забезпечення, вихід з ладу функціонування програмного забезпечення, неповне архівування даних, несанкціонований доступ.

Варто зазначити, що до захисту корпоративної інформації потрібен комплексний підхід. Використання одного чи двох методів насправді не принесе позитивного результату.

Захист реалізується програмно та адміністративно. До останнього входять [9]:

- створення внутрішнього розпорядку та підписання договорів з усіма працівниками щодо «конфіденційності» та правил користування, пересилання отриманої інформації;
- забезпечення контролю за виконанням локальних нормативно-правових актів;
- наявність ефективного методу аутентифікації з різними рівнями доступу до інформаційних таблиць;
- регулярна перевірка ефективності, та своєчасності систем управління інформаційною безпекою компанії;
- постійне резервне копіювання для відновлення ІТ-системи в разі збою, атаки або збою.

Ми визначили основні типи сучасних інтернет-загроз на підприємстві ТОВ «Глобал Вест» (рисунок 2.5), про які повинен знати кожен власник бізнесової справи і пересічний громадянин.

Завдання фішингу базується на тому, що мета зловмисника видавання себе за іншу особу полягає в тому, щоб уявити когось невірно. Отримання цінної інформації, яка може бути продана або використана для шкідливих цілей, таких як вимагання або крадіжка грошей або особистих даних. Зловмисники, які видають себе за інших, найчастіше видають себе за банки чи інші фінансові установи, щоб змусити жертву заповнити підроблену форму та отримати інформацію про рахунок.

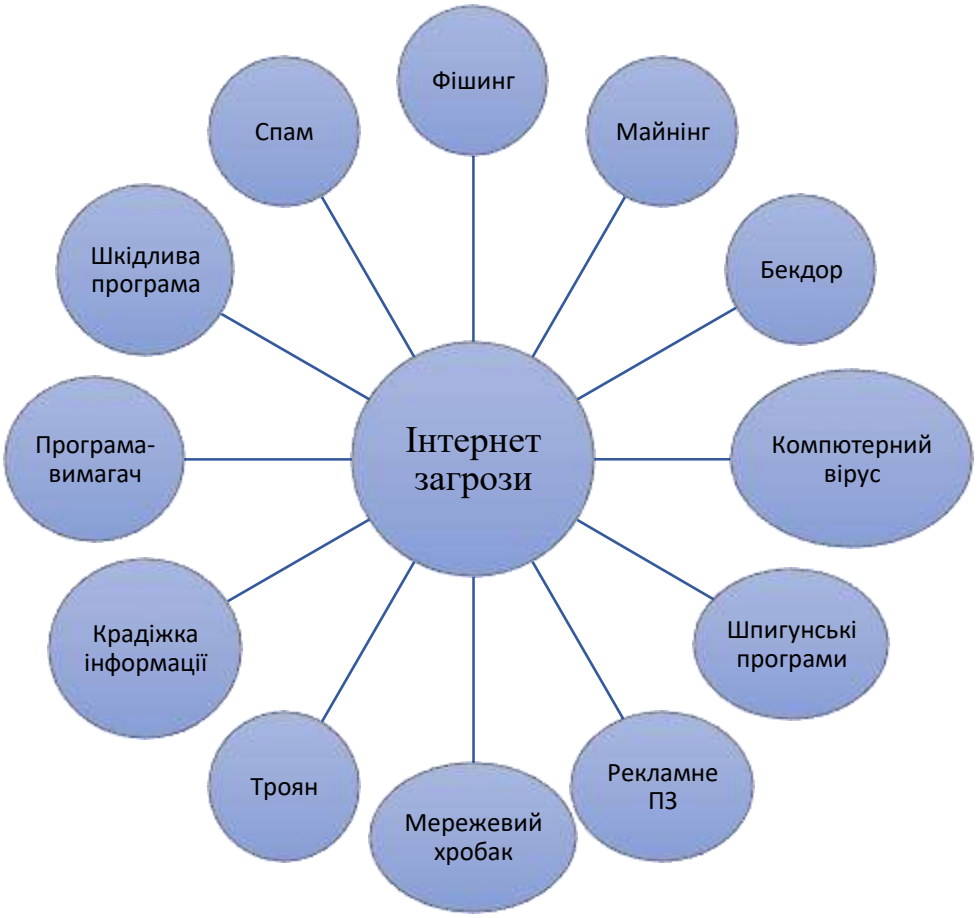


Рис.2.5 Основні типи сучасних інтернет-загроз (складено автором на основі [8])

Нелегальний майнінг використовує код, призначений для використання обчислювальної потужності певного об’єкта.

Загроза бекдор дозволяє зловмисникам контролювати інфікований пристрій жертви без дозволу та віддалено. Іноді розробники створюють їх для обходу аутентифікації або як додатковий метод доступу.

Кожен, хто знає про них або випадково їх знайде, може дістатися до них.

Іноді складно, для звичайного користувача, розуміти які саме файли в Інтернеті є шкідливими. У таких випадках існують рішення, які ідентифікують загрози за допомогою баз даних відомих небезпечних програм і за допомогою технологій захисту від нових і шкідливих програм.

Кіберзлочинці постійно шукають нові способи зараження. Зокрема, сучасні загрози поширюються через системні вразливості, обхід функцій безпеки, приховування в пам'яті або імітацію легальних програм, щоб залишитися непоміченими.

Проте більшість закладів заражені вірусами через людську недбалість, неуважність, некомпетентність керівників. Спеціально розроблені електронні листи з небезпечними доповненнями виявилися ефективним і недорогим способом входу в систему жертви. Для цього зловмисникам потрібен лише один клік.

У результаті впровадження економічних і соціальних реформ в Україні виникла нагальна потреба у формуванні та реалізації нових напрямків інвестиційної політики, спрямованої на сталий розвиток держави загалом та розвиток підприємств зокрема. Розробка інвестиційної політики базується на основі економічного зростання, створення нових ефективних механізмів залучення інвестицій, створення умов для реалізації концептуальної бази стратегії та забезпечення процесів європейської інтеграції.

Розвиток ТОВ «Глобал Вест» залежить від ефективного управління інвестиційною діяльністю, та впровадження ефективної системи інформаційної безпеки яка має носити стратегічний характер. Водночас організації діють в умовах невизначеності, нестабільного інвестиційного ринку, що впливає на кінцеві результати та прибутковість, створює загрози для забезпечення їх стабільності, підтримки фінансової стійкості, підприємницької діяльності та

прибутковості. Інвестиційна діяльність є одним із ключових факторів суспільного розвитку, оскільки забезпечує відтворення робочої сили, оновлення основних фондів виробничої та невиробничої сфер та всього процесу відтворення в економіці. Тому створення ефективних інструментів залучення інвестицій у національну економіку є найважливішою умовою сталого економічного розвитку як окремих компаній, так і економіки в цілому.

Інвестиційна політика є ключовою умовою розвитку соціально-економічних процесів і дає змогу безпосередньо впливати на темпи виробництва, забезпечувати науково-технічний прогрес, змінювати структуру суспільного виробництва та вирішувати широкий спектр стратегічних завдань [4].

Інвестиційна політика є невід'ємною частиною економічної політики держави та компаній у формі визначення структури та обсягів інвестицій, напрямів їх використання, джерел виробництва з урахуванням необхідності модернізації основних фондів та покращення їх інвестування. технічний рівень.

Механізм управління інвестиційною політикою — це сукупність основних елементів, що регулюють процес розробки та реалізації інвестиційних рішень компанії, що є запорукою сталого економічного розвитку.

Інвестиційна політика є невід'ємною частиною загальної економічної стратегії підприємства, яка визначає вибір і шляхи реалізації найбільш раціональних шляхів оновлення та розширення її виробничого та науково-технічного потенціалу. Ця політика спрямована на забезпечення виживання компанії в складних ринкових умовах, досягнення фінансової стабільності та створення умов для майбутнього розвитку. Інвестиційна політика формується лише в конкретних сферах інвестиційної діяльності підприємства, які потребують найбільш ефективного управління для досягнення основної стратегічної мети цієї діяльності [26].

Метою Політики інформаційної безпеки проведення інвестиційної політики ТОВ «Глобал Вест» є впровадження та ефективне функціонування системи управління інформаційною безпекою на підприємстві. А це, в свою чергу, забезпечить створення та безперервне обслуговування умов, за яких

ризики, пов’язані з безпекою інформаційних активів підприємства, постійно контролюються.

Виокремимо основні цілі політики інформаційної безпеки на підприємстві ТОВ «Глобал Вест»:

– Захист інформаційних ресурсів від негативного впливу зовнішніх та внутрішніх загроз, а також від вимушених або випадкових подій незбереження інформації працівників підприємства;

– забезпечення постійної та безперебійної роботи інформаційних систем в організації;

– мінімізація ризиків інформаційної безпеки;

– створення позитивної репутації про підприємство при роботі зі споживачами.

Шляхи досягнення вищезазначених цілей визначено на рис. 2.6

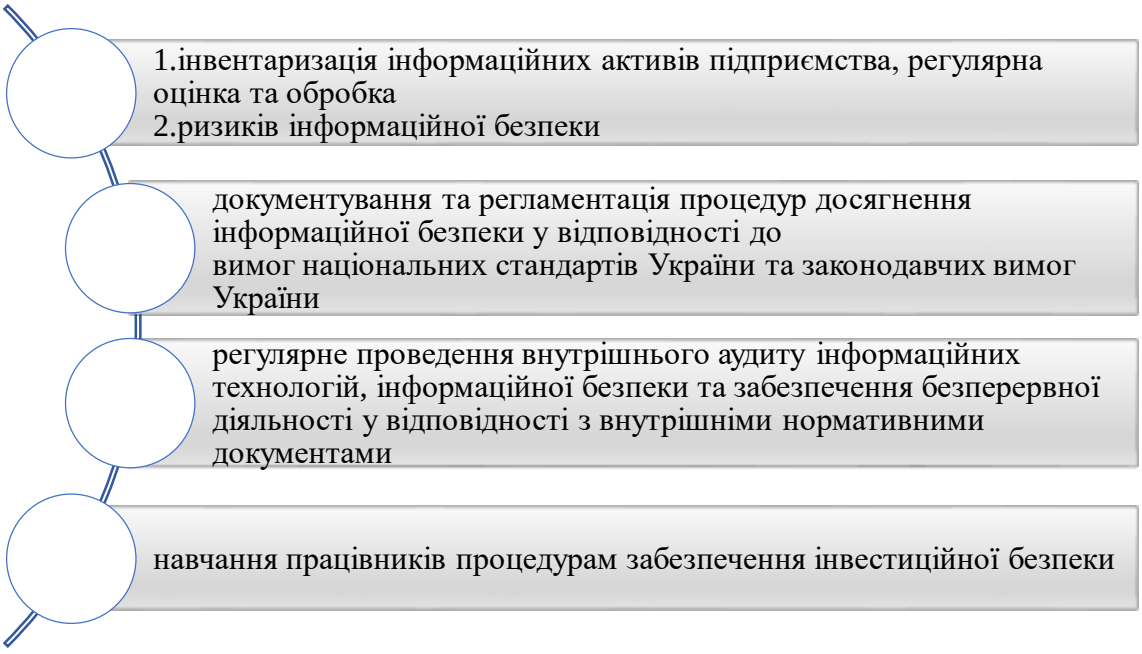


Рис. 2.6 Шляхи досягнення цілей інформаційної безпеки на ТОВ «Глобал Вест»

Ключовим завданням інформаційної безпеки на досліджуваному підприємстві є захист інформаційних ресурсів від зовнішніх та внутрішніх небезпек. Які в свою чергу можуть бути не лише вимушеними та свідомими але

й випадковими, необміркованими будь яким працівником в силу його характеру як окремої особистості.

При наданні інформаційних послуг Товариство з обмеженою відповідальністю дотримується таких принципів (рис. 2.7).

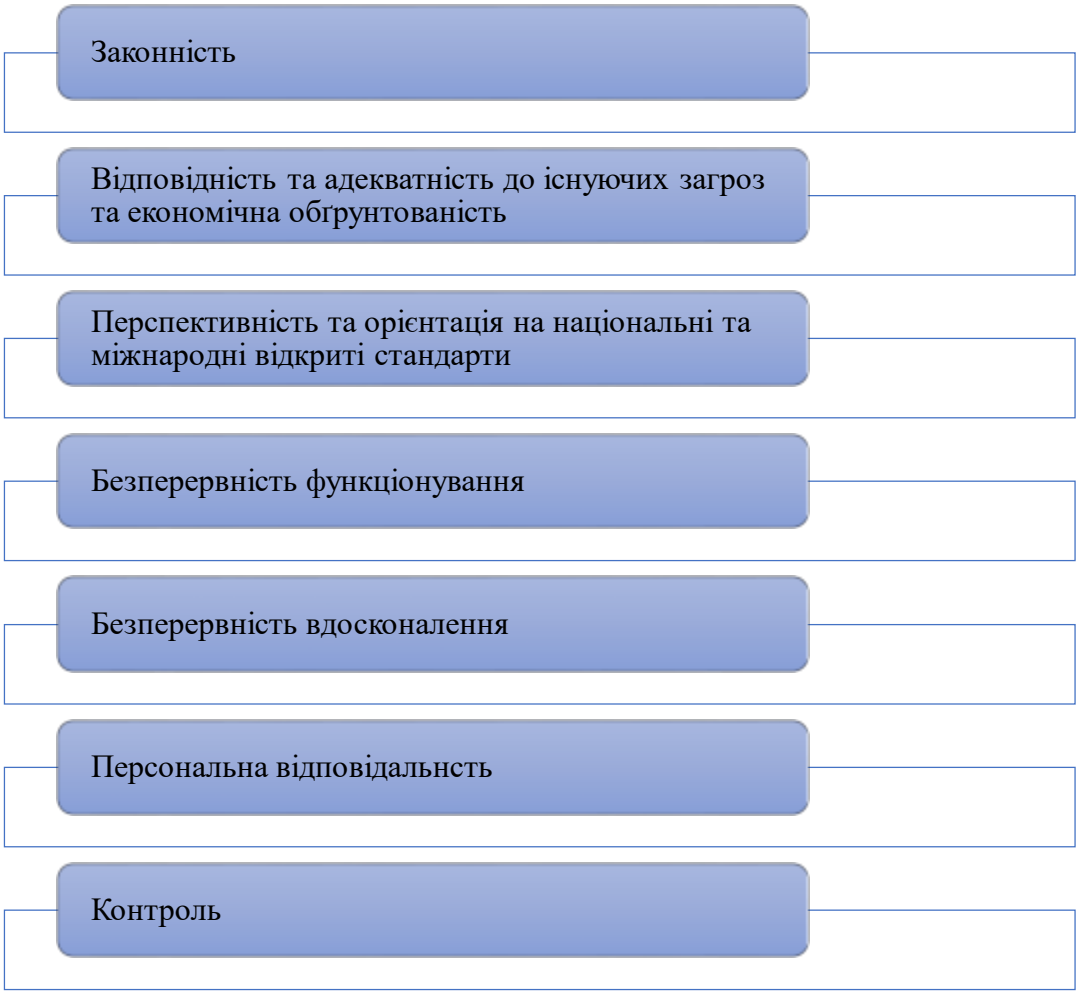


Рис.2.7 Основні принципи дотримання інформаційної безпеки при проведенні інвестиційної політики на ТОВ «Глобал Вест»

Обґрунтовуючи основні принципи дотримання інформаційної безпеки при проведенні інвестиційної політики на підприємстві зазначимо, що принцип законності свідчить про забезпечення відповідності вимогам законодавства України, нормативно-правових актів Національного банку України та інших контролюючих і регулюючих органів державної влади.

Актуальність та адекватність існуючих загроз та економічна доцільність характеризується тим, що організаційні заходи та механізми технічного захисту

будуть вибрані та застосовані виходячи з потреб бізнесу та базуються на аналізі ризиків інформаційної безпеки, зокрема на аналізі поточних загроз та витрат на впровадження та підтримку цих механізмів. Періодично проводиться оцінка ефективності впроваджених захисних заходів та механізмів.

Перспектива та орієнтація на національні та міжнародні відкриті стандарти.

Організаційно-технічні заходи інформаційної безпеки проведення інвестиційної політики на ТОВ «Глобал Вест» реалізуються з урахуванням світових тенденцій. Зосередженість на відкритих стандартах дозволяє скористатися перевагами світового досвіду в галузі інформаційної безпеки.

Принцип безперервності функціонування забезпечується надійністю, простотою, доступністю, та прозорим функціонуванням та проведенням різних організаційно-технічних заходів відносно захищеності інформації при проведенні інвестиційної політики на підприємстві .

Постійне покращення здійснюється для того щоб гарантувати інвесторам, про відсутність загрози інформаційної безпеки на підприємстві. Питання вирішуються в контексті постійних змін у внутрішньому та зовнішньому середовищі, відбувається безперервний цикл розвитку та вдосконалення системи управління інформаційної безпеки на підприємстві.

Особиста відповідальність свідчить про те, що кожен співробітник підприємства несе персональну відповідальність за виконання покладених на нього функцій та вимог в межах збереження інформаційної безпеки на підприємстві. У разі порушення вимог інформаційної безпеки, з будь яких причин працівник може бути притягнутий до дисциплінарної, матеріальної, адміністративної та кримінальної відповідальності відповідно до законодавства України.

Принцип контролю свідчить про наявність в організації ТОВ «Глобал Вест» постійного контролю за працівниками підприємства та виконанням ними основних вимог інформаційної безпеки.

Таким чином, інформаційна безпека проведення інвестиційної політики підприємства є одним із найважливіших елементів системи управління бізнесом. У процесі його розробки та реалізації визначаються пріоритетні напрями та форми інвестиційної діяльності, сутність створення інвестиційних ресурсів підприємства, послідовність етапів у досягненні короткострокових і довгострокових цілей господарюючого суб'єкта, межі інформаційної безпеки проведення інвестиційної політики на підприємстві.

2.3 Стратегічні засади забезпечення інформаційної безпеки ТОВ «Глобал Вест» у сучасному геополітичному середовищі України

Інформаційна політика у провідних країнах світу — це сукупність стратегічних принципів діяльності компетентних державних органів щодо планування та контролю процесів отримання, зберігання та поширення інформації. Крім того, наразі розвинені країни активізують державну діяльність щодо регулювання відносин в інформаційному просторі країни. З цією метою ці країни ухвалюють окремі положення щодо реалізації пріоритетних принципів інформаційної політики країни.

У сучасному глобальному геополітичному протистоянні захист внутрішнього інформаційного простору та забезпечення безпеки держави в інформаційній сфері залишаються для України незамінною темою, особливо в умовах поширення трансформаційних гібридних загроз, переважно розповсюджених державою-агресором. На цьому тлі затвердження Стратегії інформаційної безпеки [11] на національному рівні 28 грудня 2021 року є важливим і відповідальним кроком до визначення подальших можливостей для розвитку національної інформаційної сфери.

Необхідність прискорення визначення стратегічних засад забезпечення інформаційної безпеки на підприємстві обумовлюється такими викликами: ситуація у вітчизняній інформаційній сфері, яка пов'язана як із значними

інформаційними впливами, так і з втручанням російських засобів масової інформації; широке поширення російськими засобами масової інформації дезінформації про Україну; виконання спеціального інформаційного завдання Російської Федерації, спрямованого на дискредитацію та створення негативного міжнародного іміджу України у світі; у деяких регіонах нашої країни та світу існують технічні проблеми з мовленням українських електронних засобів масової інформації.

На сьогодні вітчизняний інформаційний простір має високий рівень зовнішніх загроз, які створює активна інформаційно-пропагандистська експансія Російської Федерації. Зокрема, вона прагне через інформаційну сферу впливати на політичні та соціально-економічні процеси в нашій державі, підриває авторитет законної української влади щодо деморалізації суспільства та посилення невдоволення та заперечувальних настроїв. Російська сторона також активно впроваджує технології публікації упередженої інформації в Інтернеті та засоби масової інформації, розповсюдження якої розраховане на місцевих жителів на окупованих територіях, громадян Російської Федерації та міжнародної спільноти [13].

У таких ситуаціях при вирішенні проблеми організації інформаційної безпеки особливого значення набуває її структурна класифікація, яка відносно обумовлена і побудована відповідно до конкретних цілей і припущень. З цієї точки зору доцільно поділити інформаційну безпеку за джерелами загрози на два види – безпека технічного характеру, і та що визначається соціальними факторами. Тому загрози інформаційній безпеці нині мають соціальний характер і зосереджені у внутрішньополітичній, економічній, соціальній, екологічній, інформаційній та духовній сферах нашого суспільства [12].

З метою реагування на поширення гібридних загроз в Україні, наприкінці 2021 року на державному рівні було прийнято Стратегію інформаційної безпеки як базовий документ, що визначає завдання та методи попередження криз у національному інформаційному просторі, посилення інформаційної безпеки та її елементів. Очікувалося, що практична реалізація цієї стратегії посилить

спроможність держави забезпечити власну інформаційну безпеку та захистити інформаційний простір. Росія та її інформаційна політика в цьому документі визначають основні загрози безпеці України. Стратегія має бути реалізована до 2025 року [13].

Метою цієї стратегії є підсилення спроможності надавати інформаційну безпеки держави, її інформаційного простору, забезпечення інформації та заходів соціально-політичної стабільності, захисту держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, гарантування прав і свобод кожного громадянина. Поставлена мета буде досягнута шляхом вжиття заходів щодо запобігання та придушення загроз інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій країни-агресора, спрямованих на порушення державного суверенітету, територіальної цілісності України, забезпечення інформаційної стабільності суспільства та державою створення ефективної системи співпраці органів державної влади, самоврядування та суспільства та міжнародного розвитку, співробітництво у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.

У цьому декларативному документі (Стратегія інформаційної безпеки) зазначається як важливі довгострокові цілі. Перше стосується запобігання дезінформаційно-інформаційним операціям, особливо з боку держав-агресорів проти України. Друга – забезпечення всебічного розвитку української культури та формування української громадянської ідентичності. Третє – підвищення рівня медіакультури та медіаграмотності в суспільстві. По-четверте, забезпечення поваги до права осіб на збір, зберігання, використання та поширення інформації, свободи вираження поглядів, захисту приватності, доступу до об'єктивної та достовірної інформації та захисту прав журналістів. П'ятий – ІТ-реінтеграція громадян України, які проживають на тимчасово окупованих територіях та прилеглих до України територіях, Всеукраїнський інформаційний простір. Шосте – розвиток інформаційного суспільства та підвищення культури діалогу. Сьома мета – створити ефективну систему

стратегічної комунікації. Це означає, що ці цілі створюють напрямки, які державі необхідно зміцнювати, і вони є ключовими в контексті інформаційної безпеки.

Тому до переліку загроз і викликів, які стоять перед нашою державою, і підприємствами зокрема входять: повністю експансивна інформаційна політика Російської Федерації; відносно низький рівень медіаграмотності громадян; динамічне зростання кількості глобальних дезінформаційних кампаній; інформаційне панування Російської Федерації на тимчасово окупованих територіях; використання технологій для маніпулювання обізнаністю пересічних громадян про наслідки вступу України до НАТО та ЄС тощо. Зокрема, планується, що успішна реалізація Стратегії інформаційної безпеки матиме такі позитивні наслідки, як: побудова захищеного інформаційного простору, забезпечення інформаційної безпеки держави та її складових; ефективне функціонування системи стратегічної комунікації; встановлення механізмів ефективної боротьби з поширенням нелегального контенту тощо.

Висновки до другого розділу

В другому розділі нами проведено аналіз інормаційної безпеки підприємства ТОВ «Глобал Вест» в системі проведення інвестиційної політики.

В роботі охарактеризовано діяльність Товариства з обмеженою відповідальністю «Глобал Вест». Основним видом діяльності ТОВ «Глобал Вест» є неспеціалізована оптова торгівля та її різновиди. Завдяки злагодженій роботі з командою Open Teck та додатковим інвестиціям у виробничі потужності, компанія вийшла на перше місце в списку компаній, що займаються монтажем та постачанням віконних систем в регіоні та за його межами. Open Teck є великим виробником і постачальником віконних систем і компонентів для «Глобал Вест».

В роботі визначено основну мету системи інформаційної безпеки ТОВ «Глобал Вест», яка базується на впровадженні та ефективному функціонуванні

системи управління інформаційною безпекою в компанії. Це, в свою чергу, забезпечить створення та підтримку умов для постійного моніторингу ризиків, пов’язаних із безпекою інформаційних ресурсів компанії.

В роботі виокремлено основні типи сучасних інтернет загроз, що дозволить підприємству застерегти свою інформацію, а відтак і підприємство вцілому від кібератак.

Запропоновано стратегію розвитку інформаційної безпеки інвестиційної політики ТОВ «Глобал Вест» метою якої є посилення спроможності держави забезпечити інформаційну безпеку, її інформаційний простір, інформацію та засоби соціально-політичної стабільності, захист держави, державний суверенітет, територіальну цілісність України, демократичний конституційний лад, гарантувати права і свободи кожного. громадянин.

Виокремлено основні цілі політики інформаційної безпеки в компанії «Глобал Вест» та методи їх досягнення.

Тому інформаційна безпека інвестиційної політики компанії є одним із найважливіших елементів системи управління компанією. Процес його розробки та реалізації визначає пріоритетні напрями та форми інвестиційної діяльності, характер інвестиційних ресурсів підприємства, послідовність етапів реалізації короткострокових і довгострокових цілей господарюючого суб’єкта, інформаційну безпеку, економічну безпеку, безпеки фінансової та соціальної політики, фінансової підтримки та розвитку інвестицій. інвестиційна політика в компанії.

РОЗДІЛ 3.
ШЛЯХИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ ІНВЕСТИЦІЙНОЇ ПОЛІТИКИ НА ПІДПРИЄМСТВІ

3.1 Проблеми інформаційної безпеки на ТОВ «Глобал Вест»

У своїй бізнесовій справі підприємець стикається з необхідністю обробляти, зберігати, відсортовувати, передавати та видаляти необхідну інформацію. Якщо інформація є цінною для організації то її слід захистити від зловмисників.

Психологи кажуть, що близько 25% усіх співробітників розкривають, продають або передають інформацію конкуруючим компаніям з певною метою [4].

Захист інформації в організації, або іншими словами інформаційна безпека підприємства є дуже важливим фактором його ефективного розвитку і цей фактор має бути обов'язковим. Коли підприємство укладає договір зі своїм працівником, особливо якщо цей працівник займає керівну посаду в компанії, має бути укладений договір на збереження організаційної інформації. Хоча в нашій країні система зв’язку на різних рівнях влади захищена не належним чином законодавчо.

Загалом, інформація, що зберігається в інформаційних системах компанії, є загрозою для того ж підприємства. Адже така система включає спеціальне автоматизоване програмне забезпечення, специфічні для бізнесу завдання, програмні оболонки, текстові процесори, пакети програм, бази даних, особливо з Інтернету.

Наприклад, організація «Захисту прав споживачів у кіберпросторі» виявила шкідливе програмне забезпечення, яке могло відновити роботу в українському сегменті Інтернету з 15 травня 2020 року: Яндекс, «В контакті», «Однокласники» [5]. Нещодавно хакери зламали міжнародну готельну компанію

Marriott. Особисті дані 5,2 мільйона вразливих клієнтів, включаючи імена, адреси електронної пошти та поштові адреси [6].

Питання й задачі формування стратегій інформаційної безпеки підприємства є у центрі багатьох дослідників, які наголошують на багатьох характерних рисах для таких рішень. Так, у [11] вказано, що рішення щодо безпеки приймаються на кожному рівні організації та з різних точок зору. На тактичному та оперативному рівнях організації прийняття рішень зосереджується на оптимізації ресурсів безпеки, тобто на комплексній комбінації планів, персоналу, процедур, керівних принципів і технологій, що мінімізують збитки та втрати. Хоча ці дії та тактика зменшують частоту та/або наслідки порушень безпеки, вони обмежені глобальним бюджетом організації на безпеку. На стратегічному рівні керівництво підприємства має відповісти на питання: «Що таке бюджет безпеки (витрати), де кожна гривня, витрачена на безпеку, повинна бути зважена з альтернативними витратами, не пов’язаними з безпекою, що виправдовується упущеними (попередженими) втратами і збитки?" Відповідь на це питання залежить від терпимості осіб, які приймають рішення, щодо ризику та інформації, яка використовується для його досягнення. Тобто суб’єктивний чинник відіграє суттєву роль при виборі стратегії безпеки.

Безпека бізнес-інформації є найважливішою проблемою в управлінні підприємством для управління ризиками [22]. Сучасна ера технологічної безпеки для бізнесу все більше визнається, особливо в бізнес-стратегіях. Відключення процедур інформаційної безпеки та впливу комерційних стратегічних бізнес-цілей для контролю витрат на безпеку та їх ризиків, інцидентів та втрат. Операційна корпоративна система вимагає узгодження практик безпеки шляхом вбудовування управління ризиками інформаційної безпеки в організацію, однак вона стикається з серйозними проблемами для підтримки та забезпечення діяльності бізнесу. Безпека узгодження в бізнес-процесах є однією з найбільших проблем у гарній організації, оскільки вона потребує ресурсів підтримки та управління часом, а також способів узгодження безпеки для подолання бізнес-цілей. Таким чином, роль управління інформаційною безпекою є важливою в

якості керівництва для виконання інформаційної безпеки бізнесу. Крім того, систематичне управління безпекою впроваджує бізнес-модель захисту критичної інформаційної інфраструктури.

При захисті інформації необхідно перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на всіх наявних у компанії носіях. Загрози інформаційної безпеки можна розділити на внутрішні та зовнішні.

Зовнішні злоякісні дії можуть виглядати так:

- копіювання цінних документів або крадіжка файлів;
- крадіжка флеш-карт;
- крадіжка інформації в процесі її передачі через Інтернет;
- пошкодження носіїв інформації;
- надання інформації конкурентам або, загалом, іншій країні;
- крадіжка інформації у інсайдерів;
- залучення працівників до іншої компанії.

Найпоширенішими внутрішніми загрозами є крадіжка та зараження інформаційними вірусами або пошкодження файлів працівниками компанії. Причинами внутрішніх загроз ТОВ «Глобал Вест» є:

- причини психологічного характеру у зв'язку з нерозвиненістю взаємовідносин між працівниками підприємства;
- невдоволення рівнем заробітної плати;
- погані відносини між працівником і керівництвом.

Для забезпечення інформаційної безпеки компанії необхідно посилити права зареєстрованих користувачів, якими можуть бути фізичні особи та організації. Ці користувачі можуть виконувати лише заздалегідь визначені дії за допомогою інформаційних технологій.

Небезпека інформації в компанії походить з певних джерел (рис.3.1)

При аналізі завдання інформаційної безпеки ми вводимо поняття обчислювального середовища, в якому дані обробляються за допомогою комп’ютерних програм. Дані та обчислювальні програми знаходяться на внутрішніх носіях. Під операційним середовищем ми розуміємо набір елементів

обчислювального середовища, які знаходяться в операційній системі комп'ютера. Захист елементів обчислювального середовища практично зводиться до захисту даних і програм. Заходи захисту інформації включають захист елементів обчислювального середовища та контроль елементів операційного середовища.

Рис. 3.1 Основні джерела загроз інформаційної безпеки ТОВ «Глобал Вест»

Захист обчислювального середовища включає:

- захист даних;
- забезпечує власні програми безпеки;
- захист процедур обробки інформації.

Контроль елементів робочого середовища включає:

- контроль зовнішніх компонентів операційного середовища;
- перевірка цілісності внутрішніх елементів операційного середовища;
- контроль семантики даних.

Захист інформації здійснюється різними способами. Нижня частина містить захист програми проти читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу та виконання програм, самотестування та самовідновлення виконуваного програмного коду.

Питання авторського права – це питання інтелектуальної власності, яке є пріоритетним для розробників програмного забезпечення. Захист від копіювання забезпечується програмним забезпеченням, яке використовує ідентифікацію користувача, обмежує кількість запусків програми, обмежує кількість запусків або обмежує кількість запусків. Самоперевірка та самовідновлення програмного коду здійснюється шляхом впровадження діагностичних модулів функцій програмного коду. Це розмір файлу, список контрольних точок, контрольна сума, слабкі технічні засоби обробки інформації; неякісне програмне забезпечення для обробки інформації; засоби зв'язку, охорони, сигналізації; інші технічні засоби, що використовуються в установі.

Алгоритми також використовуються для повернення до стандартного програмного коду, якщо це необхідно.

Тому в умовах сьогодення інформаційна безпека в компанії означає постійний контроль над джерелами потенційних загроз (антропогенні, технологічні та природні ресурси) та необхідність захисту інформації різними способами (захист програм від зчитування та копіювання, захист авторські та активні програми, самотестування).

3.2 Принципи інформаційної безпеки процесу інвестиційної політики підприємства ТОВ «Глобал Вест»

Сьогодні бізнес не може бути успішним без використання сучасних технологій. Тому на перший план виходить інформаційна (IT) безпека компанії.

Інформаційна безпека – це комплекс заходів, які захищають інформацію від фішингу, будь-якого несанкціонованого шпигунського доступу, завантаження чи зміни даних, що призводять до «збою» або збою в роботі різних систем.

Традиційна інформація сьогодні втрачає цінність. Натомість медіа, кібер- та цифровий контент стають все більш актуальними.

Кіберзлочинці можуть атакувати не тільки відомі корпорації, а й малий і середній бізнес, який обробляє інформацію про кредитні картки або зберігає певну конфіденційну інформацію (Рис.3.2).

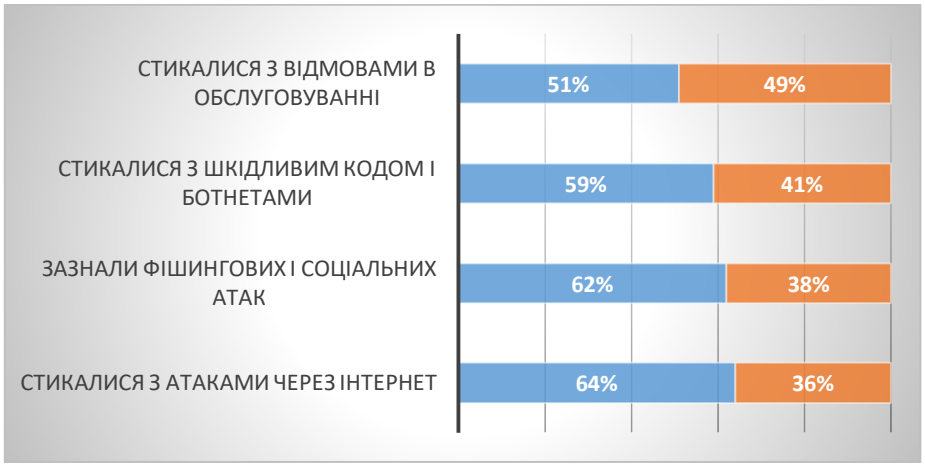


Рис. 3.2 Порушення інформаційної безпеки підприємствами, за 2021рік

Багато власників бізнесу роблять велику помилку, коли хочуть заощадити на інформаційній безпеці, тому що вони не піклуються про захист даних, припускаючи, що їм байдуже. Однак інструменти кіберзлочинців постійно вдосконалюються, а кількість жертв збільшується.

Однак найпоширенішою причиною порушень кібербезпеки є людська недбалість (рис. 3.3)

Рис. 3.3 Основні причини порушення інформаційної безпеки на ТОВ «Глобал Вест»

Тому, щоб захистити свій бізнес від неправдивої інформації, менеджер, а то і кожен працівник н підприємстві повинні дотримуватися наступних правил проти кібератак:

По перше, своєчасно та достовірно інформуйте своїх співробітників про поточні зміни в організації, загрозу банкрутства або перспективи розвитку. Кіберзлочинці зазвичай намагаються отримати доступ до даних організації через її «найслабкішу точку», недосвідченого персоналу. Спочатку зловмисники надсилають фейковий звіт, настільки справжній, що співробітник не дізнається про шкідливу роботу і відкриває його. Тоді сценарії різні: пристрій завантажується вірусами, троянами, шпигунськими або іншими шкідливими програмами. Тому першим кроком у зміцненні інформаційної безпеки в організації має стати інформування працівників про поточні загрози та заходи захисту від них. Кожен співробітник повинен усвідомлювати необхідність захисту даних компанії та даних клієнтів. Бізнес-директори повинні регулярно проводити тренінги з інформаційної безпеки в усіх відділах (маркетинг, продажі, кол-центр тощо), які займаються політикою інформаційної безпеки та захисту даних, тим, як можна атакувати зловмисників і як їх уникнути.

По друге, захистіть свій комп'ютер і носій інформації. Незахищені дані піддаються комерційним кібератакам і шкідливому програмному забезпеченню. Тому що в разі втрати чи крадіжки фірмових флешок, ноутбуків чи смартфонів працівник розкриває всі дані компанії. Щоб запобігти подібним ситуаціям, ми рекомендуємо: Завжди виходити з системи та джерел, які містять конфіденційні дані, і не залишати комп’ютер увімкненим. Шифруйте всі ваші бізнес-дані за допомогою рішення для шифрування, яке дозволяє віддалено керувати ключами шифрування та встановлювати правила для файлів, жорстких дисків, знімних дисків, карт пам’яті та електронних листів. В результаті, якщо функціональний пристрій буде втрачено, зловмисники не зможуть прочитати дані компанії; регулярно створюйте резервні копії файлів. Це дозволить вам отримати інформацію в будь-який час.

По третє, надійний контроль в організації. Адже з міркувань безпеки підприємства негласні дані повинні зберігатися на окремих серверах, які забезпечують додатковий захист через брандмауери або інші служби безпеки. Це зменшує ризик викрадення даних. Вам також потрібно стежити за користувачами, які здійснюють покупки або намагаються отримати доступ до вашої мережі. Це дозволяє адміністраторам швидко виявляти підозрілу поведінку та реагувати на неї.

По четверте, надійна співпраця. Кожна угода про надання послуг, постачання або іншу співпрацю має містити конкретні вимоги безпеки. Багато постачальників хмарних послуг регулярно переглядають різні заходи щодо загроз, щоб відповідати галузевим стандартам інформаційної безпеки. Постачальник послуг повинен мати рівень безпеки, відповідний партнерству.

Захист віддаленого доступу. Високошвидкісний доступ до Інтернету та сучасна трудова етика в організації дозволяють багатьом офісним працівникам працювати з дому.

Такий режим роботи з року в рік стає все більш популярним. Особливо сьогодні можливість безпечної дистанційної роботи для компаній є великою перевагою.

Кожен співробітник або клієнтський пристрій, що забезпечує віддалений доступ до корпоративної мережі, повинен відповідати стандартам інформаційної безпеки.

У сучасному представленні ролей функції служби інформаційної безпеки можна виокремити чотири ключових напрямки:

перше – розробка методології та методів аналізу загроз, оцінка рівня інформаційної безпеки компанії та системи її безпеки;

друге, організація та здійснення спеціальних заходів із захисту інформації;

третє – підтримка технічних засобів захисту інформації;

четверте – аудит і контроль системи інформаційної безпеки компанії.

Тому будь-яка компанія, яка зберігає та обробляє дані користувачів, може бути атакована. Однак, якщо дотримуватися всіх правил інформаційної безпеки,

підприємство матиме значно менше втрат і мінімальну кількість помилок у бізнес-процесах.

3.3 Пропозиції вдосконалення інформаційної безпеки інвестиційного процесу на підприємстві

Розвиток глобального інформаційного процесу суспільства, який спостерігається в останні десятиліття, є наслідком регіональної проблеми інформаційної безпеки. Сьогодні багато важливих інтересів компанії багато в чому визначаються станом інформаційного середовища. Цілеспрямований або ненавмисний вплив на інформаційну безпеку із зовнішніх або внутрішніх джерел може завдати чималої шкоди цим інтересам і створити загрозу та ризик для безпеки.

Не випадково питання інформаційної безпеки вже давно є пріоритетом майже всіх великих компаній. Останнім часом все більше керівників малого та середнього національного бізнесу усвідомлюють реальну небезпеку, пов’язану з конфіденційною інформацією, системами її обробки та залученими в цей процес працівниками.

ТОВ «Глобал Вест» використовує ризиковий підхід для розуміння, моніторингу та зменшення операційних ризиків. Деталі ризик-орієнтованого підходу описані в окремому внутрішньому документі підприємства.

Усі працівники підприємства обізнані та дотримуються вимог інформаційної безпеки на роботі.

При розробці, впровадженні та експлуатації програмно-технічних засобів враховуються вимоги інформаційної безпеки.

ТОВ «Глобал Вест» забезпечує дотримання всіх вимог інформаційної безпеки, встановлених угодами з третіми сторонами щодо участі в міжнародних системах платежів і переказів грошей.

З метою зниження ризику інцидентів, пов’язаних з інформаційною безпекою, керівництво підприємства створює умови для систематичного навчання працівників інформаційної безпеки.

Періодично підприємство розробляє, підтримує, тестує та оновлює плани дій на випадок непередбачених критичних ситуацій.

Щоб вибрати засоби боротьби з кіберзагрозами, потрібно чітко розуміти особливості свого бізнесу:

- наявність відгалужень, потрібен віддалений доступ і доступ до глобальної мережі передачі даних;
- рівень логістики та актуальності обладнання (воно здатне «отримати» новітнє програмне забезпечення);
- всі блоки потребують максимального захисту або лише деякі потребують захисту;
- наявність/відсутність ІТ-відділу та рівень компетентності його персоналу;
- достатньо забезпечити безпеку інформації на комп’ютері в організації, або контролювати мобільні пристрої персоналу, оскільки вони також передають конфіденційні дані.

Для того щоб підприємство ТОВ «Глобал Вест» не стало ціллю кіберзлочинця які обробляють дані кредитних карток або зберігають певну конфіденційну інформацію ми пропонуємо основні правила необхідного забезпечення інформаційної безпеки підприємства:

1. Покращення обізнаності персоналу

Як правило, кіберзлочинці намагаються отримати доступ до даних компанії через «найслабше місце» підприємства – недосвідчений персонал. Спочатку зловмисники надсилають фейкове повідомлення, яке настільки реальне, що співробітник не підозрює зловмисну діяльність і відкриває його. Далі сценарії різні - пристрій завантажується програмами для шантажу, троянами, шпигунськими або іншими шкідливими програмами.

2. Захист робочих пристроїв персоналу та фізичних носіїв

Незахищені дані піддають компанії кібератакам і зараженню шкідливим програмним забезпеченням. Тому що якщо корпоративні USB-накопичувачі, ноутбуки чи смартфони будуть втрачені або вкрадені, ви скомпрометуєте всі свої корпоративні дані. У гіршому випадку, якщо він потрапить в чужі руки, це може призвести до шантажу злочинців, які шукають викуп. Щоб уникнути таких ситуацій, ми пропонуємо:

• ніколи не забувати виходити з системи та ресурсів, які містять конфіденційні дані;

• шифрувати чи ставити на пароль всі бізнес-дані за допомогою рішення для шифрування, яке дозволяє віддалено керувати ключами шифрування та встановлювати правила для файлів, жорстких дисків, знімних дисків, карт пам'яті та електронної пошти. В результаті, якщо функціональний пристрій буде втрачено, зловмисники не зможуть прочитати дані компанії;

• регулярно копіювати файли в резерв. Це дозволить відновити дані в будь-який момент.

3. Періодично але часто прослідковувати мережі та користувачів, які намагаються увійти.

Існує багато причин сегментації корпоративної мережі, а саме зниження навантаження на систему, контроль доступу та безпека. З міркувань інформаційної безпеки конфіденційні дані повинні зберігатися на окремих серверах, які забезпечують додатковий захист через брандмауери або інші служби безпеки. Таким чином створюється ряд бар’єрів, які знижують ризик викрадення даних. Крім того, необхідно відстежувати користувачів, які здійснюють покупки або намагаються отримати доступ до вашої мережі. Це дозволяє особам, які здійснюють догляд, швидко виявляти будь-яку підозрілу поведінку та реагувати на неї.

4. Співпраця з перевіреними постачальниками

Сучасні технології значно спростили систему комунікації між організаціями, що відкриває нові можливості для партнерів і полегшує відносини між компаніями. Однак це спричинило іншу проблему. Кіберзлочинці почали

атаки на малий бізнес, щоб отримати доступ до більш цінних корпоративних даних.

Кожна угода про надання послуг, постачання чи іншу співпрацю має містити конкретні вимоги безпеки. Багато постачальників хмарних послуг регулярно проходять перевірку на наявність різних загроз на відповідність стандартам інформаційної безпеки в певній сфері діяльності.

Найголовніше, що постачальник послуг повинен мати рівень безпеки, який вам підходить. Якщо для систем підприємства та партнерських служб немає належного захисту, ви можете зробити необхідні запити.

5. Сформувати віддалений доступ до мережі компанії.

Високошвидкісний доступ до Інтернету та сучасна трудова етика дозволяють багатьом офісним працівникам працювати з дому. З року в рік такий режим роботи набуває все більшої популярності. Особливо сьогодні можливість безпечної дистанційної роботи є величезною перевагою для компаній.

Будь-який пристрій співробітника або клієнта, що забезпечує віддалений доступ до корпоративної мережі, повинен відповідати стандартам інформаційної безпеки, які вимагають:

− підключення до віртуальної приватної мережі (VPN).

− використовуйте двофакторну аутентифікацію під час входу або підключення до VPN.

− доступ до віртуальної машини як варіант підключення за замовчуванням, якщо це можливо.

− використовуйте комплексне рішення безпеки для захисту від зловмисників, шпигунського програмного забезпечення та інших загроз, а також запобігання фішинговим атакам.

Таким чином, для того щоб ТОВ «Глобал Вест» не стало жертвою хакерської атаки потрібно дотримуватися всіх правил інформаційної безпеки. Тоді компанія матиме значно менші збитки та неполадки бізнес-процесів.

Експерти з інформаційної безпеки мають дві думки. По-перше, інформаційну безпеку в компанії взагалі неможливо інтегрувати без витрат. У

цьому випадку цілком можливо, що прийнятний ризик цілком виправданий. Другий погляд: витратити частину грошей на створення системи інформаційної безпеки або витратити частину грошей на навчання персоналу, програмне забезпечення тощо, забезпечуючи таким чином достатній рівень безпеки. Проте також будуть певні прогалини, які рано чи пізно призведуть до витоку чи крадіжки конфіденційної інформації.

Таким чином, у сучасних умовах інформаційна безпека є невід'ємною складовою економічної безпеки суб'єкта господарювання. Надійна інформаційна безпека є передумовою переходу до моделі сталого розвитку не лише окремого підприємства, а й усієї національної економіки. На нашу думку, особливу увагу слід приділити реальній реалізації запропонованих заходів із забезпечення інформаційної безпеки, що має бути покладено в основу розробки та реалізації інформаційної політики підприємства з метою захисту інформації від внутрішніх та зовнішніх загроз.

Висновки до третього розділу

В третьому розділі нами розглянуто шляхи вдосконалення інформаційної безпеки проведення інвестиційної політики на підприємстві.

Виокремлено основні проблеми та принципи і напрямки інформаційної безпеки на підприємстві. Запропоновано підприємству дотримуватись усіх правил інформаційної безпеки. Тоді компанія матиме значно менші збитки та неполадки бізнес-процесів.

Визначено внутрішні та зовнішні загрози інформаційної безпеки на підприємстві ТОВ «Глобал Вест» враховуючи його внутрішню організаційну структуру та вплив зовнішніх факторів на підприємство.

Кожен співробітник або клієнтський, що забезпечує віддалений доступ до корпоративної мережі, повинен відповідати стандартам інформаційної безпеки.

Тому будь-яка компанія, яка зберігає та обробляє дані користувачів, може бути атакована. Однак при дотриманні всіх правил інформаційної безпеки підприємство матиме значно менше втрат і мінімальну кількість помилок у бізнес-процесах.

У сучасних умовах інформаційна безпека є невід'ємною частиною економічної безпеки суб'єкта. Надійна інформаційна безпека є необхідною умовою переходу до моделі сталого розвитку не лише окремої компанії, а й усієї національної економіки. Нами визначено, що особливу увагу слід приділити фактичному виконанню запропонованих заходів із забезпечення інформаційної безпеки, що має бути основою для розробки та реалізації інформаційної політики підприємства у сфері захисту інформації від внутрішніх та зовнішніх загроз.

ВИСНОВКИ

У кваліфікаційній роботі досліджено, що комунікація є невід’ємною частиною процесу управління. Може об'єднати окремі елементи організації в одну мету, що дозволяє координувати їх діяльність, аналізувати успіхи та невдачі, виправляти помилки, ставити нові завдання; його зв’язок із зовнішнім середовищем – вони надаватимуть інформацію про стан ринку та поведінку підприємців, інформуючи ділових партнерів та споживачів про їхні наміри та впливаючи на їх поведінку.

Тому без обміну інформацією жодна організація не може функціонувати повноцінно. Оскільки дослідження проблеми та шляхів удосконалення комунікації в системі управління є надзвичайно важливим завданням, комунікація не обмежується єдиною інформацією.

Таким чином організаційна комунікація має відбуватися в різних напрямках - всередині і за межами організації, на одному управлінському рівні (по горизонталі) і між рівнями (по вертикалі) по діагоналі, якщо обговорення того, як вирішити проблему, стосується відповідних суб'єктів і без обмежень. і є неформальним. Кожна з цих форм спілкування виконує свою роль і дотримується певних правил. В останні десятиліття важливість технологічних аспектів менеджменту була основною сполучною ланкою між цілями, принципами лідерства та економічними механізмами. Без технологічної підтримки керівник повинен кардинально змінитися в результаті комп’ютеризації, ефективні рішення не можуть бути реалізовані важливими людьми.

Нами визначено, що корпоративна інформаційна безпека є системою захисту корпоративної інформації; захист від крадіжки, передчасне і неточне пред'явлення одержувача. Нехтуючи засобами масової інформації, підприємець може зазнати значних збитків або взагалі втратити бізнес.

Ми запропонували основні принципи інформаційної безпеки в компанії, завдяки яким керівник може бути впевнений, що його компанія інформаційно захищена.

В роботі визначено основну мету системи інформаційної безпеки ТОВ «Глобал Вест», яка базується на впровадженні та ефективному функціонуванні системи управління інформаційною безпекою в компанії. Це, в свою чергу, забезпечить створення та підтримку умов для постійного моніторингу ризиків, пов'язаних із безпекою інформаційних ресурсів компанії.

Запропоновано стратегію розвитку інформаційної безпеки інвестиційної політики ТОВ «Глобал Вест» метою якої є посилення спроможності держави забезпечити інформаційну безпеку, її інформаційний простір, інформацію та засоби соціально-політичної стабільності, захист держави, державний суверенітет, територіальну цілісність України, демократичний конституційний лад, гарантувати права і свободи кожного громадянина. Це буде досягнуто шляхом вжиття заходів щодо запобігання та послаблення загроз інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій з боку агресора, спрямованих на порушення державного суверенітету, територіальної цілісності України, забезпечення інформаційної стабільності та налагодження ефективної системи взаємодії між органів державної влади, місцевого самоврядування та суспільства, а також міжнародного розвитку, співробітництва у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.

У роботі висвітлено основні типи сучасних інтернет-загроз, які дозволять компанії захистити свою інформацію, а отже і компанію в цілому, від кіберпростору. А також виокремлено основні цілі політики інформаційної безпеки та шляхи їх реалізації.

Для того щоб підприємство ТОВ «Глобал Вест» не стало ціллю кіберзлочинця які обробляють дані кредитних карток або зберігають певну конфіденційну інформацію в роботі запропоновано основні правила необхідного забезпечення інформаційної безпеки підприємства.

Таким чином інформаційна безпека інвестиційної політики компанії є одним із найважливіших елементів системи управління підприємством. Процес його розвитку та реалізації найбільш доцільних напрямів і форм інвестиційної діяльності, характер інвестиційних ресурсів підприємства, відповідно етап реалізації короткострокових і довгострокових підрозділів суб'єкта господарювання, інформаційна безпека, економічність. безпеки, фінансового забезпечення та соціальної політики, фінансової підтримки та розвитку інвестицій інвестиційна політика в компанії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блага Н.В. Удосконалення комунікаційних процесів на підприємстві у контексті зміцнення інформаційної безпеки URL:http://dspace.lvduvs.edu.ua/handle/1234567890/3986

2. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство і право.* 2004. №3. С.88-91

3. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи. Вісн. Хмельниц. нац. ун-ту. 2010. № 2. Т. 2. С. 32–35.

4. Крюков О.І. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво*. 2007. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12

5. Громадська організація «З захисту споживачів у кіберпросторі». Офіційний сайт: URL: https://bezbid.com/news/poperedzhennya-pro-zagrozu-kiberbgigiyeni/

6. Центр інформаційної та технічної підтримки в Україні. Компанія ESET. Офіційний сайт URL: https://www.eset.com/ua/

7. Закон України «Про інформацію» Офіційний сайт URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

8. Блага Н. Дослідження інформаційної безпеки комунікаційного процесу на підприємстві. Актуальні проблеми зміцнення економічної безпеки держави та суб'єктів господарської діяльності: матеріали всеукраїнської науково-практичної конференції (м. Львів, 16 квітня 2021р.) за заг.ред. В.С.Бліхара. Львів : Львівський державний університет внутрішніх справ, 2021 С.19-22.URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/16_04_2021.pdf

9. Інформаційна безпека підприємства: методи захисту від головних загроз. URL: https://group-fs.com/informaczijna-bezpeka-pidpryyemstva-metody-zahystu-vid-golovnyh-zagroz/

10. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємництва: навч. посіб. Київ: МАУП, 2006. с.134 с.

11. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпе- ки, методи та засоби боротьби: підручник. Київ: ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

12. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: автореф. дис. .канд. юрид. наук: спеціальність 12.00.07. Львів. 2019. 23 с.

13. Золотар О.О. Правові основи інформаційної безпеки людини: автореф. дис. ...д-ра юрид. наук: спеціальність 12.00.07. Харків. 2018. 37 с.

14. Указ Президента України від 28.12.21 р. No 685/2021. 2. Довгань О.Д., Ткачук Т.Ю. URL: https://www.president.gov.ua/documents/6852021-41069

15. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. № 1(24)/2018. С. 89-103. Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 411 с.

16. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий журнал. 2020. № 2. С. 200-203.

17. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. Інвестиції: практика та досвід. 2019. № 11. С. 123-127.

18. СамохваловЮ.Я., Браіловський М.М. Оцінка інформаційної безпеки організації за критерієм впевненості. Захист інформації. 2019. Т. 21. № 1. С. 13-24.

19. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Резонанс. 2017. № 18. С. 3-14. URL: http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf

20. Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & security*, 27(1-2), 22-29. DOI: 10.1016/j.cose.2008.03.002

21. Fakhri, B., Fahimah, N., & Ibrahim, J. (2015). Information security aligned to enterprise management. *Middle East Journal of Business*, 55(1593), 1-5.

22. Axelrod, C. W., Bayuk, J. L., & Schutzer, D. (2009). *Enterprise information security and privacy.* Artech House.

23. Coyne, E. J., & Davis, J. M. (2007). *Role engineering for enterprise security management.* Artech House, Inc..

24. Про захист персональних даних: Закон України від 1.06.2010 № 2297-VI станом на 13.02.2022р.

URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

25. Top 10 Global Business Risks for 2016. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2016.pdf

26. Литвинов В.В. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. пос. Чернігів: Чернігів. нац. технол. ун-т, 2016. 254 с.

27. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 411 с.

28. Золотар О.О. Правові основи інформаційної безпеки людини: автореф. дис.д-ра юрид. наук: спеціальність 12.00.07. Харків. 2018. 37 с.

29. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: автореф. дис. канд. юрид. наук: спеціальність 12.00.07. Львів. 2019. 23 с.

30. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. Інформація і право. № 3(15), 2015. С. 36-42.

31. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Резонанс. 2017. № 18. С. 3-14. URL: http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf

32. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. Юридичний вісник. № 3. 2019. URL: https://lexinform.com.ua/dumka-eksperta/doktryn alni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti

33. Самохвалов Ю.Я., Браіловський М.М. Оцінка інформаційної безпеки організації за критерієм впевненості. Захист інформації. 2019. Т. 21. № 1. С. 13-24.

34. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. Інвестиції: практика та досвід. 2019. № 11. С. 123-127.

35. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий журнал. 2020. № 2. С. 200-203.

ДОДАТКИ

Додаток А

Найпоширеніші види порушень із боку персоналу організації:

- фальсифікація сум готівки у касі та коштів на банківських рахунках, підробка фінансових документів підприємств;
- несанкціонований продаж і використання майна підприємства з корисливою метою;
- оплата роботи підставних (фіктивних) осіб;
- фальсифікація документації підприємства за допомогою електронної техніки та Інтернету;
- несанкціоновані операції з цінними паперами, матеріальними й нематеріальними активами підприємства;
- повідомлення конфіденційної та іншої інформації третім особам;
- фальсифікація звітів про використання коштів, виділених на відрядження, представницькі видатки, на інші потреби підприємства;
- порушення техніки безпеки та правил внутрішнього трудового розпорядку.

Бодаток Б

Задля попередження загроз кадровій безпеці потрібно планувати й організовувати заходи для її забезпечення в усіх напрямах кадрової політики організації.

Ці заходи повинні включати:

- аналіз причин виникнення негативних впливів на персонал
- оцінку поточного рівня кадрової безпеки в організації
- виявлення «білих плям»
- пошук шляхів виходу з проблемного стану
- бюджетне планування досягнення кадрової безпеки організації
- розрахунок ефективності запропонованих заходів організації
- оперативну реалізацію запропонованого комплексу заходів у процесі діяльності організації.

Для збереження кадрової безпеки доцільно використовувати сучасні кадрові технології, включаючи такі механізми, як:

- ефективна мотивація
- прискорена адаптація (завдяки наставництву)
- забезпечення контролю з боку служби персоналу
- своєчасне запобігання конфліктним ситуаціям
- атестація
- компенсація
- розумна політика звільнення
- пропаганда корпоративності