МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.27.14.000 КРБ

Козак Микита Олексійович

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: **«Комп'ютерна інженерія»**

Група: **2БКС-27**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему:

«Дослідження рівня безпеки малих підприємств з розробкою захисних мір»

Проектний матеріал складається з пояснювальної записки на 66 сторінках та графічного (презентаційного) матеріалу на 12 аркушах (слайдах)

Виконавець _____ (Козак М.О.)

Керівник проекту _____ (Кільдішев В.Й.)

Консультанти:

з охорони праці _____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувачка кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «26» 06 2023 р. Протокол ДКК № 3

Оцінка ДКК 4 (добре)

Секретар ДКК _____

АНОТАЦІЯ

Метою даної роботи є аналіз методів та засобів щодо захисту малих підприємств.

У бакалаврській роботі розглянуто роль малих підприємств в рамках держави. Розглянуто загрози та ризики підприємств малого бізнесу (ПМБ) - як внутрішні, так і зовнішні. Наведено ризикоутворюючі фактори виникнення загроз. В рамках застосування засобів захисту запропоновано використання антивірусів та іншого захисного програмного забезпечення.

Ключові слова: малий бізнес, захист, підприємство.

ANNOTATION

The purpose of this paper is to analyze the methods and means of protecting small enterprises.

The bachelor's thesis examines the role of small enterprises within the state. The threats and risks of small businesses (SMEs), both internal and external, are considered. The risk factors of threats are presented. The use of antiviruses and other security software is proposed as part of the application of protection measures.

Keywords: small business, protection, enterprise.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Кафедра *комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"_____" _____ 202____ р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти Козаку Микиті Олексійовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Дослідження рівня безпеки малих підприємств з розробкою захисних мір

затверджена наказом по коледжу від *17 жовтня 2022 р. № 235-А2-ОД*

2. Термін здачі кваліфікаційної роботи

3. Вихідні дані до роботи Об'єкт аналізу – підприємство «АртСталь». Аналіз існуючих захисних мір. Антивірусні програми. Програми захисту доступу до мережі. Розробка захисних мір.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Вступ. 1. Технологічний розділ. 2. Охорона праці. Висновки. Перелік використаних джерел. Додаток А

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Лист 1 – Проблеми малого бізнесу

Лист 2 – Внутрішні загрози. Вплив війни на малий бізнес

Лист 3 – Зовнішні загрози

Лист 4 – Рекомендації щодо захисту малих компаній

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів роботи, що стосується їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Кільдішев В.Й.*		
Охорона праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 03.02.2023р.

Керівник роботи *Кільдішев В.Й.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1	Узяти за основу підприємство (приватної власності), розписати його структуру	**27.05.2023 р.**	Виконано
2	Особливості роботи малого бізнесу в реаліях війни	**02.06.2023 р.**	Виконано
3	Зловмисники та їхні дії	**04.06.2023 р.**	Виконано
4	Способи захисту підприємств від хакерських атак	**08.06.2023 р.**	Виконано
5	Виконання розділу «Охорона праці»	**13.06.2023 р.**	Виконано
6	Чистове оформлення пояснювальної записки кваліфікаційної роботи	**15.06.2023 р.**	Виконано
7	Підготовка доповіді та презентації для захисту	**17.06.2023 р.**	Виконано
8	Отримання рецензії, відповіді на зауваження рецензента	**21.06.2023 р.**	Виконано
9	Захист роботи	**до 30.06.2023 р.**	Виконано

Виконавець _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27.14.000 КРБ	*Кваліфікаційна робота*		
А4			*БКС 27.14.000 КРБ ПЗ*	*Пояснювальна*		
				записка		

Зм.	Арк.	№ докум.	Підпис	Дата	*БКС 27.14.000 КРБ ПЗ*		
Розробив		Козак М.О.			Дослідження рівня безпеки малих підприємств з розробкою захисних мір	Літ.	Аркуш 4 / Аркушів 66
Перевірив		Кільдішев В.Й.					
Н. Контр.		Петрашова В.І.				ОТФК ОНТУ гр.БКС-27	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Підприємства малого бізнесу відіграють значну роль в економіці країни. Бізнес залежний від інтернету, який таїть у собі безліч загроз. Не варто забувати і про внутрішні загрози: витік даних, вразливості у використовуваному програмному забезпеченні, шпигунство тощо. Весь спектр зовнішніх і внутрішніх загроз ставить перед невеликими компаніями непросте завдання зі створення системи IT-безпеки, яка дасть змогу ефективно протистояти сучасним загрозам.

Якщо міркувати про інформаційну безпеку малого бізнесу, найкраще підійде таке визначення: щоб стати ціллю, зовсім не обов'язково бути ціллю. Будь-яка компанія може стати жертвою атаки і потрапити в складну ситуацію з вкраденими даними. Чомусь керівники малого бізнесу нерідко відмахуються від проблем інформаційної безпеки з аргументом «кому ми потрібні»? Компанія, може й ні, а дані про клієнтів, постачальників, угоди, платежі - цілком.

Невеликі компанії приватного бізнесу далеко не завжди працюють у сфері торгівлі. У цьому форматі створюється більшість інноваційних, впроваджувальних, наукових підприємств, що займаються актуальними розробками. І інтерес конкурентів до їхніх рішень здатен призвести до організації навмисних витоків.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Типи організаційних структур малих підприємств

Організована робота в компанії - запорука її розвитку. Щоб створити порядок і чітко розподілити працю на підприємстві, потрібно сформувати правильну організаційну структуру.

Логічна система, яка пов'язує функціональні підрозділи, відображає внутрішню структуру підприємства - це називають організаційна структура підприємства.

Організаційна структура - це матриця розподілу функцій в організації, яка встановлює зв'язки між підрозділами та розділяє відповідальність між ними для досягнення бізнес-цілей. Правильна організація структури дає змогу співробітникам будь-яких рівнів реалізувати свій потенціал і працювати максимально ефективно.

Організаційна структура підприємства регулюється комплексом документів:

- **Положення про організаційну структуру** - регламентуючий документ, який описує всі підрозділи та їхні функції.
- **Положення про структурні підрозділи**. Документ складається за необхідності деталізувати роботу підрозділів, щоб не навантажувати основне положення.
- **Посадові інструкції**. Описують усі функції та обов'язки кожної посади.
- **Організаційна схема (оргсхема).** Вона в графічному вигляді представляє оргструктуру і дає можливість швидко зрозуміти, як влаштована організація.

Приклад організаційної схеми:

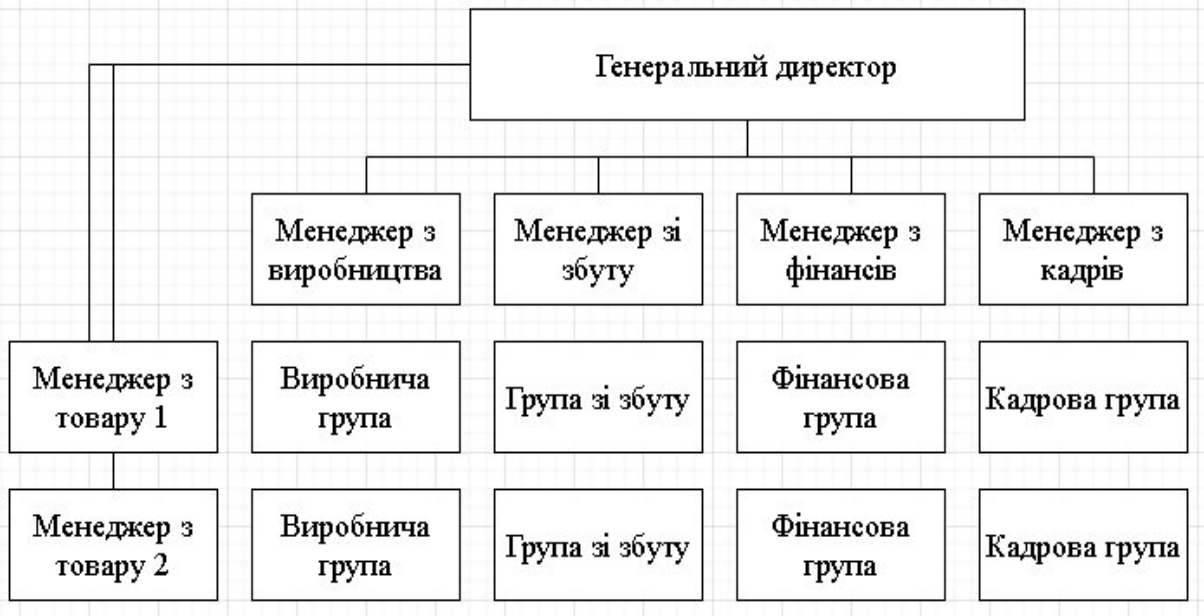


Рисунок 1.1 - Приклад організаційної схеми

Організаційна структура має значення для всіх співробітників компанії - вона служить сполучною ланкою між членами команди, організовує їхню роботу. Розглянемо окремо переваги організаційної структури для керівників і для лінійних співробітників.

Користь для керівників

- **Чітка система управління**. Найчастіше співробітники закріплюються за функціями, але не несуть відповідальності за кінцевий результат. Оргструктура усуває цю проблему - позначаються зони відповідальності кожного підрозділу і кожної посади.
- **Раціональний розподіл навантаження**. В організації без оргструктури функції часто розподілені стихійно. Тому одні співробітники перевантажені, а в інших багато вільного часу. Опис бізнес-процесів допомагає сформувати структурні підрозділи з оптимальним штатом і завантаженістю кожного.
- **Систематизація процесу найму**. Розроблені посадові інструкції дають розуміння, які фахівці потрібні в компанію, і якими знаннями та компетенціями вони повинні володіти.

Користь для співробітників

Співробітнику організаційна структура підприємства допомагає:

- **Швидше познайомитися** з компанією під час працевлаштування, зрозуміти масштаб бізнесу. З'ясувати, до кого і з якими питаннями звертатися.
- **Зрозуміти свою роль** в організації, побачити цінність своєї роботи. Розібратися як відбувається загальний бізнес-процес і взаємодіють різні відділи компанії.
- **Визначити**, де закінчується зона відповідальності його відділу і починається зона відповідальності інших підрозділів
- **Побачити кар'єрні перспективи** - які можливості для вертикального та горизонтального зростання є в організації.

Структурний підхід включає в себе кілька етапів до побудови організаційної структури:

Створення організаційної структури - започаткування формальної системи правил, що уможливлює контролювати взаємодію співробітників фірми.

Методи розподілу функціональних обов'язків залежать від закладених у правила розподілу підстав: розмір груп, виконувані функції, територія, вид продукції, що випускається.

Відбір способу передання повноважень полягає в централізації та децентралізації структури управління.

1.1.1 Обрання типу організаційної структури

Обрання типу організаційної структури полягає в побудові ієрархічної структури, в якій штатні одиниці пов'язані між собою правом віддавати розпорядження.

У будові управління фірмою виникають горизонтальні зв'язки, які мають характер узгоджень. Вертикальні зв'язки, або зв'язки підпорядкування,

виникають за наявності кількох рівнів управління. Вертикальні зв'язки можуть бути лінійними та функціональними.

Організації мають різну організаційну структуру, залежить від того, чим вони займаються. Для кожної компанії розробляється індивідуальна оргструктура, але в її основі використовують типові форми.

Основні види організаційних структур:

1.1.2 Лінійна структура

Лінійна організаційна структура - найпростіший вид. Вона застосовується у випадках, коли виконувана робота одноманітна і не складна; власник організації постійно спостерігає за роботою персоналу. Розпорядження швидко спускаються зверху вниз і призводять до оперативних ефективних дій. Завдяки тому, що кожен співробітник підпорядкований тільки одному керівнику, і пов'язаний з вищим керівництвом тільки через керівника або помічника. У лінійній структурі чітко відображена відповідальність, вона забезпечує швидкість реакції на прямий наказ. Важлива відмінність від інших схем - відсутність структурних підрозділів.

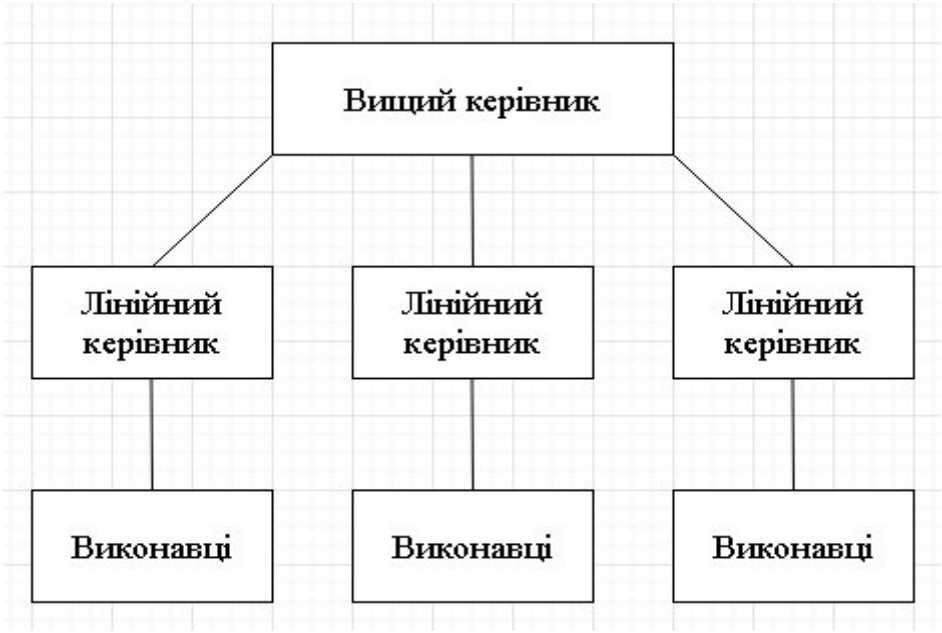


Рисунок 1.2 - Лінійна структура

Лінійна структура управління використовується дрібними і середніми фірмами, у яких не складне виробництво.

1.1.3 Функціональна структура

Зі зростанням виробництва та обсягів виникає необхідність делегувати свої повноваження - або повністю, або деякі функції. Вона підходить для великих фірм, з великою кількістю співробітників і з однаковими видами діяльності. Функціональна організаційна структура дає змогу передавати відповідальність функціональним керівникам, не втрачаючи при цьому контроль і зберігаючи вертикаль влади.

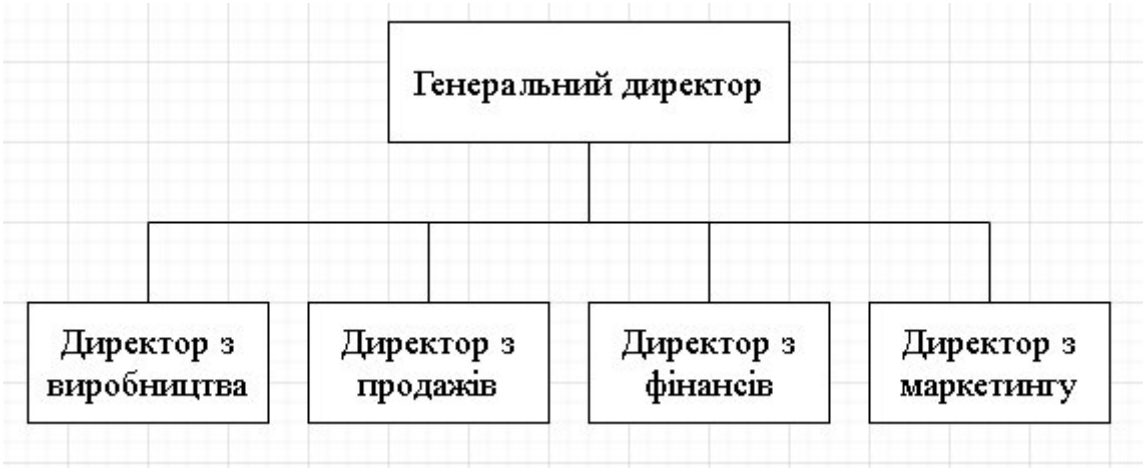


Рисунок 1.3 - Функціональна структура

Функціональна структура бізнесу передбачає поділ усієї організації на явні елементи з власними завданнями і функціями. Застосування такої схеми управління характерне для організацій, яким властива стабільність зовнішніх умов.

1.1.4 Дивізійна структура

Великі компанії застосовують дивізійну структуру управління, яка дає змогу усунути недоліки функціональної структури управління бізнесом.

Сюди відносять види організаційних структур, які групують співробітників за різними підрозділами (дивізіонами). Наприклад, підрозділи

можуть бути за типом продукції (продуктова структура) або регіоном (регіональна структура). Якщо підприємство виробляє чотири лінійки продукції, у нього буде чотири підрозділи. Або, якщо вона представлена в трьох регіонах, у неї буде три підрозділи. Кожен дивізіон працює самостійно.

Такий підхід дає змогу розвантажити зайнятих на високій посаді керівників, звільнивши від необхідності витрачати час на вирішення робочих завдань. Завдяки цьому можна отримати досить високу ефективність роботи. Такий вид організаційної структури використовується багатьма великими корпораціями. Однак важливо розуміти, що створення надто довгого ланцюжка команд призводить до некерованості.

Рисунок 1.4 - Дивізійна структура

1.1.5 Матрична структура

Суть матричних структур - у створенні тимчасових робочих груп у вже діючих структурах. Керівник групи отримує працівників і ресурси інших підрозділів у подвійне підпорядкування.

Створення тимчасових груп дає змогу більш ефективно реалізувати проєкти, а також з більшою гнучкістю розподіляти кадри. До недоліків підходу відносять складну структуру і високу ймовірність виникнення конфліктів.

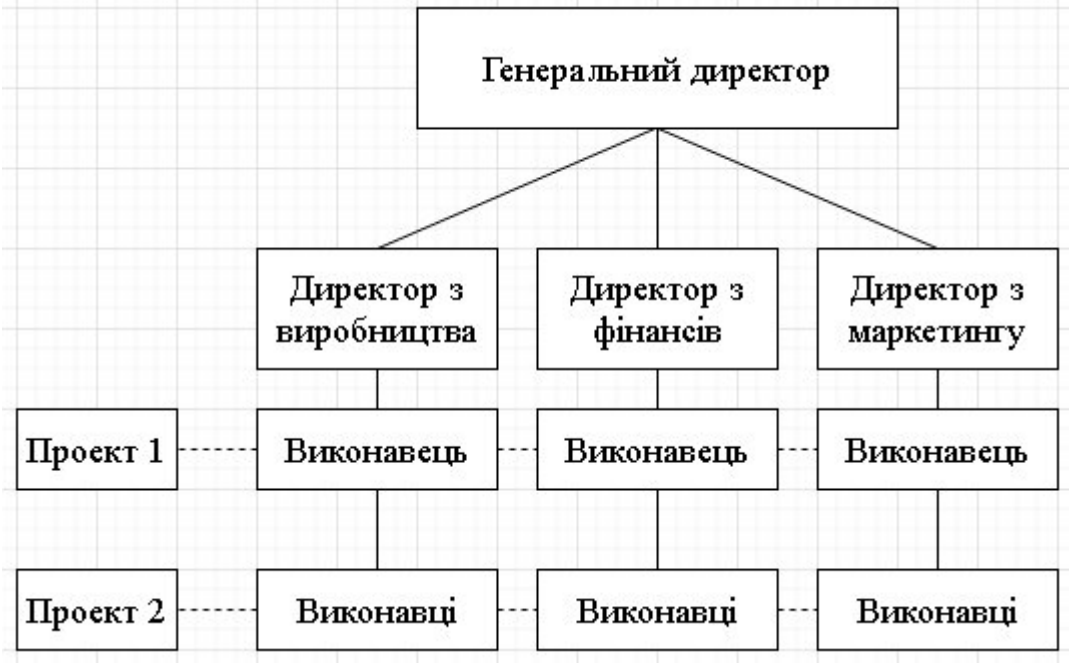


Рисунок 1.5 - Матрична структура

Це комбінація функціональної та дивізійної структури. Співробітники перебувають у подвійному підпорядкуванні (горизонтальному і вертикальному) - за функцією і за проєктом. Матрична організаційна структура довела ефективність під час реалізації нових проєктів, вона дає змогу гнучко розподіляти людські ресурси. За кожним проєктом стежить окремий менеджер, але його права сильно обмежені - в основному займається розподілом ресурсів. Основна відповідальність за проєкт - на керівнику підрозділу.

1.1.6 Організаційна структура управління: особливості побудови

Управління бізнесом відбуватиметься максимально ефективно, якщо організація структури підібрана правильно. Під час створення структури управління важливо намагатися створювати менше рівнів управління та найкоротший ланцюг команд.

Основні вимоги до організаційних структур:

- організаційна структура має відображати цілі та завдання;
- потрібно оптимізувати поділ праці між управлінцями й окремими; співробітниками, забезпечити оптимальне навантаження, а також належну спеціалізацію;
- пов’язувати організаційну структуру з поясненням обов'язків і відповідальності кожного співробітника, з визначенням горизонтальних і вертикальних зв'язків між працівниками та управлінцями;
- потрібно підтримувати відповідність між обов'язками та відповідальністю, щоб система управління працювала злагоджено;
- якщо на одному підприємстві структура управління працює ефективно, це не означає, що вона підійде і для іншої фірми.

Принципи організаційної структури в сучасних ринкових фірмах:

- рівновага прав і відповідальності;
- ясність цілей для всіх підрозділів;
- простота і чіткість структури управління;
- координація відповідальності на вищому рівні управління фірмою;
- гнучкість фірми відповідно до динаміки ринку.

Підбиваючи підсумок, слід зазначити, що коли перестає діяти структура управління в організації або вона від самого початку не підходить, необхідно її замінити на більш відповідну. Для цього потрібно правильно сформулювати цілі та завдання. Вони мають бути максимально визначальними, щоб нова структура дала змогу організації краще взаємодіяти із зовнішнім середовищем, розподіляти і спрямовувати зусилля працівників, задовольняти суспільні потреби, досягати своїх цілей.

Для того щоб створити успішну структуру управління потрібно:

- скоротити розміри підрозділів і замінити їх на кваліфікованих фахівців;
- зменшити кількість ступенів управління;
- задовольнити потребу ринку;

- зосередити співробітника на здійсненні своїх здібностей;
- створити бізнес-центри;
- миттєво реагувати на зміну;
- поліпшити горизонтальні зв'язки всередині організації;
- удосконалення інформаційних технологій;
- зміцнити зв'язки з покупцем;
- поліпшити якість продукції.

1.1.7 Аналіз та оцінка управління малим бізнесом на прикладі малого підприємства «АртСталь»

Загальна характеристика підприємства малого підприємства:

Мале підприємство «АртСталь» перебуває на ринку вже понад 10 років. Джерелом фінансування підприємства є власні кошти. Підприємство займається виробництвом та оптовим продажем кованої продукції. В організації працює близько 10 осіб.

Основними видами діяльності є:

- виробництво виробів з металопрокату та кованих виробів;
- розробка та проектування огорож;
- реалізація елементів кованої продукції;
- торгово-закупівельні та заготівельні операції на договірній основі з підприємствами, організаціями.

У процесі своєї діяльності організація ухвалює низку рішень:

- яку продукцію або номенклатуру товарів слід випускати та продавати;
- на які ринки потрібно виходити з цим товаром і як закріпити свої позиції на ринку;
- які матеріали придбати та як їх використовувати;
- як розподіляти фінансові ресурси;

- яких показників організація хоче і повинна досягти щодо технічних характеристик товару, що випускається, його якості, ефективності виробництва.

Форма продажу продукції:

- зустріч покупців;
- пропозиція продукції та їхній показ;
- допомога у виборі;
- складання замовлення та договору;
- розрахунок.

Якщо клієнт хоче індивідуальний ескіз, то на це йде від 1-4 днів. Виконання замовлення залежить від його обсягу та складності.

У торгівлі важлива оперативно-організаційна діяльність, спрямована на здійснення процесів купівлі-продажу товарів для задоволення попиту та отримання прибутку.

Важливим у діяльності всього підприємства є:

- закупівля матеріалів;
- виробництво виробів;
- товарні запаси та асортимент;
- продаж;
- реклама.

Основні проблеми у керівників:

- як взяти на роботу співробітників, від яких буде мінімум неприємностей;
- як все встигати і щоб якість була на висоті.;
- чим мотивувати співробітників, щоб вони добре працювали;
- як розподіляти роботу між співробітниками;
- як вирішувати конфлікти;
- як не підірвати здоров'я тощо;
- швидкість виконання роботи не менш важлива, ніж її зміст;

- співробітників потрібно відбирати і навчати;
- платити потрібно за кінцевий результат, а не за діяльність.

1.1.8 Аналіз структури управління «АртСталь»

На чолі «АртСталь» стоїть генеральний директор, який координує діяльність усієї організації. У його компетенції перебувають усі питання поточної діяльності підприємства.

Лінійна структура управління «АртСталь»: нижчестояще ланка (підрозділ, працівник) повністю підпорядковується вищестоящій керівнику. Генеральний директор «АртСталь» створив апарат із заступників, які готують проєкти рішень, що вимагає від генерального директора професіоналізму під час процесу ухвалення рішення.

У лінійній структурі управління «АртСталь» рішення передаються по ланцюжку зверху - вниз, сам працівник управління підпорядкований безпосередньо начальнику, а начальник підпорядкований уже генеральному директору. Тут діє принцип єдиноначальності, суть полягає в тому, що працівник виконує розпорядження тільки одного керівника. В ідеалі генеральний директор не має права віддавати розпорядження будь-яким виконавцям, обходячи стороною їхнього безпосереднього начальника.

1.2 Інформаційна безпека малих підприємств

Підприємства малого бізнесу відіграють значну роль в економіці країни. Бізнес залежний від інтернету, який таїть у собі безліч загроз. Не варто забувати і про внутрішні загрози: витік даних, вразливості у використовуваному програмному забезпеченні, шпигунство тощо. Весь спектр зовнішніх і внутрішніх загроз ставить перед невеликими компаніями непросте завдання зі створення системи IT-безпеки, яка дасть змогу ефективно протистояти сучасним загрозам.

Якщо міркувати про інформаційну безпеку малого бізнесу, найкраще підійде таке визначення: щоб стати ціллю, зовсім не обов'язково бути ціллю. Будь-яка компанія може стати жертвою атаки і потрапити в складну ситуацію з вкраденими даними. Чомусь керівники малого бізнесу нерідко відмахуються від проблем інформаційної безпеки з аргументом «кому ми потрібні»? Компанія, може й ні, а дані про клієнтів, постачальників, угоди, платежі - цілком.

Невеликі компанії приватного бізнесу далеко не завжди працюють у сфері торгівлі. У цьому форматі створюється більшість інноваційних, впроваджувальних, наукових підприємств, що займаються актуальними розробками. І інтерес конкурентів до їхніх рішень здатен призвести до організації навмисних витоків.

Крім патентів і результатів досліджень цінність для конкурентів можуть мати такі категорії даних:

- стратегічні плани розвитку компанії;
- унікальні бізнес-процеси;
- інформація про ключових співробітників;
- персональні дані клієнтів (наприклад, для фірм, що працюють у сфері медицини).

Як показує практика, зі зломами і витоками стикається безліч компаній. Навіть великі компанії та технологічні гіганти не здатні запобігти всім атакам на корпоративні середовища - на жаль, сучасні зловмисники добре прокачані та

часто у своїх методах випереджають найдосконаліші системи протидії злому та витокам.

1.2.1 Проблематика малого бізнесу

Малий бізнес, на відміну від великих компаній, не вважає пріоритетним завдання розроблення чіткої стратегії розвитку IT-інфраструктури свого підприємства, на перше місце ставлять продуктову, операційну або маркетингову діяльність. Звідси і виникають проблеми, пов'язані з інформаційною безпекою. Важливою причиною є відсутність кваліфікованого персоналу, в рідкісних випадках невеликі компанії можуть похвалитися наявністю в штаті IT-фахівця. Зазвичай його функції виконує досвідчений користувач з-поміж штатних співробітників або, в кращому разі, системний адміністратор, що приходить. Багато невеликих компаній не мають штатного фахівця з IT, тому про окремого фахівця з ІБ навіть і мови йти не може. Як правило, такі організації працюють за принципом «поки грім не вдарить», адже превентивно оцінювати можливі ризики IT-безпеки просто нікому. У кращому разі питаннями інформаційної безпеки займається IT-відділ або внутрішня служба безпеки.

Згідно з нещодавнім дослідженням «B2B International» 96% опитаних IT-фахівців невірно оцінюють швидкість появи нових загроз, лише 4% опитаних дали близьку до реальності оцінку.

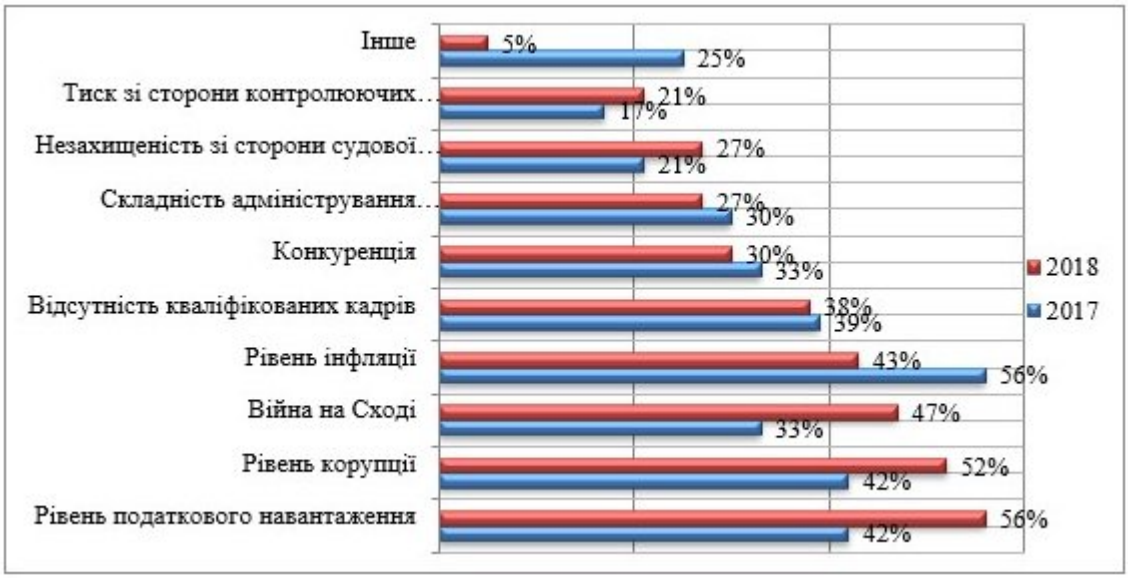


Рисунок 1.6 - Проблеми малого бізнесу. Дані за 2017 та 2018 роки

У невеликих компаніях керівна ланка не надає особливої значущості питанням інформаційної безпеки, вважаючи кіберзагрози несуттєвим ризиком для бізнесу, і, як наслідок, виділяє недостатньо часу і коштів на вирішення питань безпеки. Обмеженість бюджету змушує компанії переходити на безкоштовне або неліцензійне програмне забезпечення. Особливо гостро проблема відсутності коштів і використання неліцензійного програмного забезпечення відчувається в регіонах. Антивірусні бази, що не оновлюються тижнями, з огляду на блокування ліцензії захисного програмного забезпечення - стандартна картина для маленької фірми.

Пересилання електронних повідомлень, пошук нових клієнтів і партнерів у мережі, використання IM-месенджерів і соціальних мереж для спілкування і, що найважливіше, використання банк-клієнтів для проведення фінансових операцій - так виглядає робочий день у невеликій компанії.

Навчання персоналу компанії основам роботи з IT-системами особливо важливе, оскільки людський фактор нерідко відіграє вирішальну роль під час проведення атаки на компанію. Однак у 2013 році інтерес до інвестицій у навчання персоналу роботі з IT-системами знизився на 7%.

За даними досліджень, загрози інформаційної безпеки вважають одним зі своїх головних бізнес-ризиків, які посилилися в реаліях війни агресивними діями з боку зловмисників.

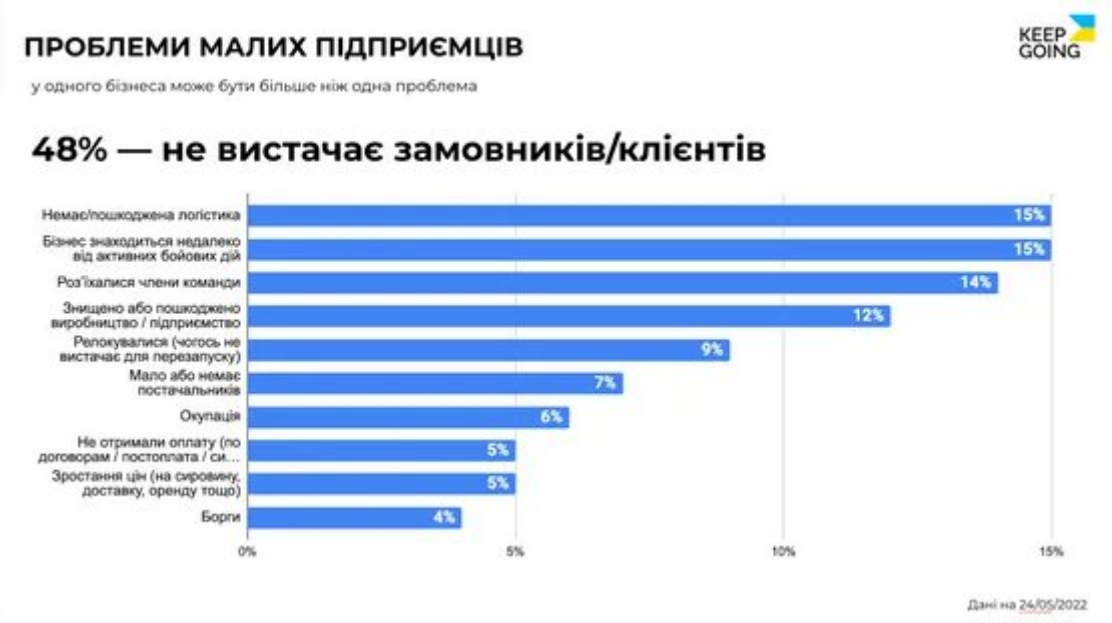


Рисунок 1.7 - Проблеми малого бізнесу. Дані за 24 травня 2022 року

З наявних недоліків систем забезпечення безпеки можна припустити таке:

- недостатня увага та нехтування загрозами до комерційної інформації;
- помилкова впевненість у співробітниках і надійності інфраструктури;
- брак фінансових ресурсів або надмірна економія на витратах;
- відсутність кваліфікованих фахівців;
- неможливість систематичного оцінювання та коригування інформаційної безпеки організації.

Ситуація у сфері безпеки малого бізнесу ускладнюється відсутністю нормативів, що враховують особливості цього сектору бізнесу в галузі інформаційної безпеки. Тому доцільно вивчити зарубіжний досвід у цій сфері. Національним інститутом стандартів і технологій США (NIST) видано рекомендаційний документ.

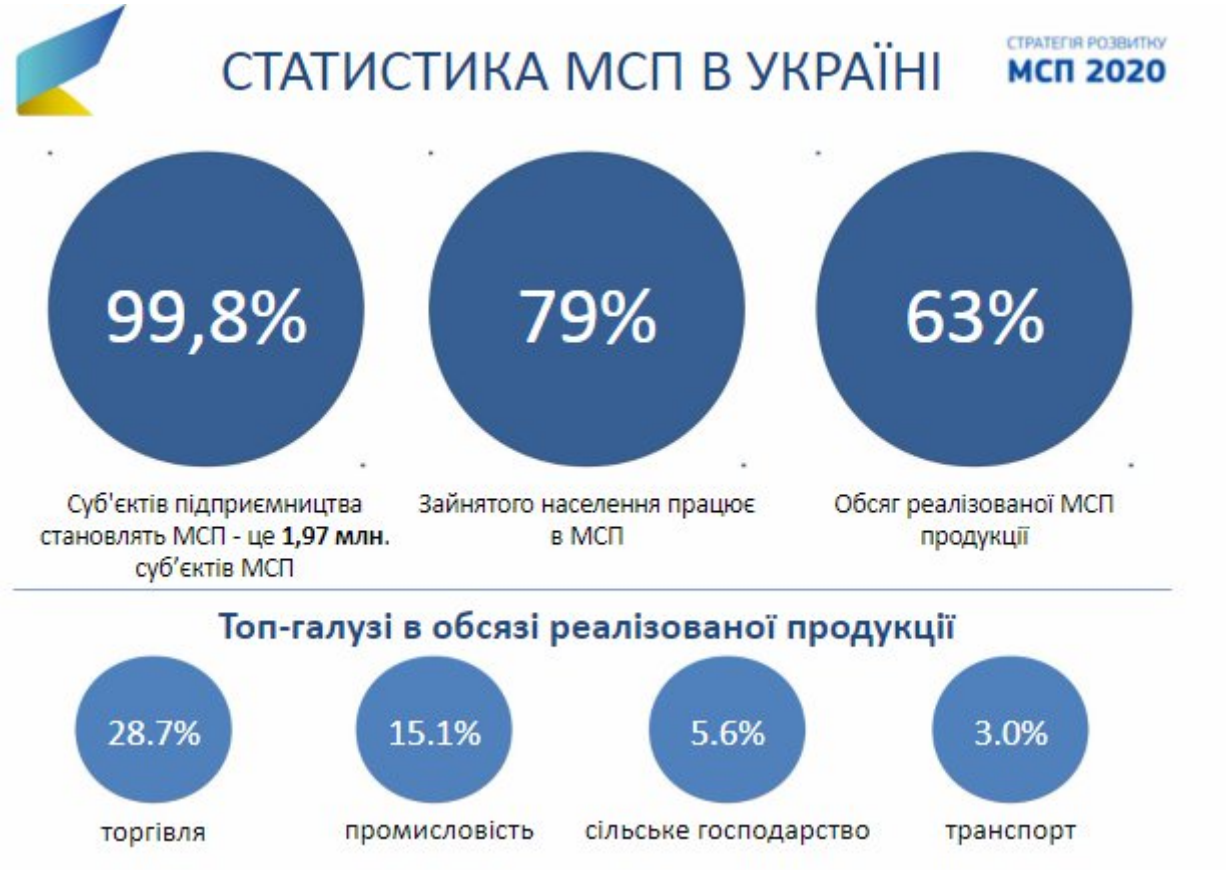


Рисунок 1.8 - Статистика малого та середнього бізнесу. Дані за 2020 рік

У ньому вказуються такі «абсолютно необхідні» дії щодо забезпечення безпеки підприємств малого бізнесу:

- захист інформації, систем або мереж від вірусів, шпигунських програм та іншого шкідливого коду;
- забезпечення безпеки під час підключення до мережі Інтернет;
- встановлення та налаштування програми засобів захисту ЕОМ;
- своєчасне оновлення операційних систем і додатків;
- регулярне резервне копіювання важливих для бізнесу даних та інформації;
- розмежування фізичного доступу до комп'ютерів і мережевих комунікацій;
- захист бездротових мереж і точок доступу;
- навчання співробітників основним принципам забезпечення безпеки;

- створення окремих облікових записів користувачів для кожного співробітника на робочих комп'ютерах і для бізнес-додатків;
- розмежування доступу співробітників до даних та інформації й обмеження повноважень для встановлення програмного забезпечення.

Також хочеться звернути увагу на те, що в цьому документі особлива увага приділяється загрозам, пов'язаним із людським фактором. Якщо в рамках програмного та апаратного захисту більшістю підприємств застосовуються хоча б мінімальні заходи, то цю частину загроз, як правило, ігнорують. Так, під час найму співробітників необхідно з'ясувати, щонайменше, чи не мали вони судимостей, також, за можливості, бажано зв'язатися з колишніми роботодавцями претендента.

Необхідно приділити увагу і захисту від соціальної інженерії. Соціальна інженерія є способом особисто або дистанційно отримати неавторизований доступ до інформації, систем, послуг або важливих аспектів діяльності підприємства, маніпулюючи людьми. Соціальний інженер досліджує організацію, щоб дізнатися імена, посади, обов'язки та публічно доступну особисту ідентифікаційну інформацію. Потім соціальний інженер зазвичай використовує отримані дані на підприємстві та за допомогою правдоподібних, але вигаданих відомостей, намагається переконати персонал, що хтось (зловмисник) пов'язаний з організацією та потребує інформації або доступу до систем, які працівник організації може надати, при цьому у працівника створюють відчуття, що він зобов'язаний зробити це. Для захисту від соціальної інженерії співробітники мають бути спеціально проінструктовані.

1.2.2 Внутрішні загрози

Уразливості в програмному забезпеченні, витік даних або крадіжка мобільних пристроїв співробітників компанії приносить великий головний біль фахівцям з інформаційної безпеки. Для мінімізації інцидентів, пов'язаних із внутрішніми погрозами, на середніх і великих підприємствах використовують програмно-апаратні DLP-системи, які дають змогу здійснювати комплексні

заходи щодо запобігання витоку даних із компанії. Шифрування ділового листування, папок і файлів, контроль знімних носіїв - невеликий перелік дій необхідних для мінімізації витоку даних. Керування оновленням програмного забезпечення - один із ключових аспектів внутрішньої безпеки, оскільки переважна більшість атак починається з експлуатування вразливостей у ПЗ.

Рисунок 1.9 - Як війна вплинула на малий бізнес. Дані за березень 2022 року

Так у 2010 році, використовуючи вразливість у браузері Internet Explorer, було здійснено атаку на низку відомих світових компаній, зокрема корпорація Google повідомила про факт отримання кіберзлочинцями доступу до поштових серверів Gmail. Прикладів таких атак маса, зловмисники отримують доступ не тільки до даних клієнтів компаній, а й до конфіденційних даних самої компанії.

Цікавою особливістю є той факт, що компанії часто дбають про новітні вразливості, але забувають про старі проломи, які досі використовуються для атак. Аналіз великих інцидентів у минулому, найчастіше свідчить про те, що в них не були використані вразливості нульового дня. На цю тему було проведено спеціальне дослідження.

Домінуючою концепцією останніх кількох років стає використання особистих мобільних пристроїв співробітників у робочих цілях, так званий BYOD (Bring Your Own Device). Сучасний бізнес заохочує мобільність співробітників, роблячи їх більш лояльними, дозволяючи перебувати поза офісом і виконувати робочі завдання. Використання власних пристроїв породжує додаткові IT-ризики для компаній, нові пристрої перетворюються на точки доступу до корпоративної інфраструктури.

Існує кілька підходів для забезпечення безпеки під час використання BYOD:

- VDI (Virtual Desktop Infrastructure) - технологія дає змогу організувати доступ до робочих місць, використовуючи спеціальні додатки або операційні системи, запущені у віртуальному середовищі на серверах організації. Підхід забезпечує централізоване адміністрування та зберігання даних.
- MDM (Mobile Device Management) - програмне забезпечення для доступу до корпоративної інфраструктури з мобільних пристроїв.
- Клієнтське ПЗ безпеки - клієнт на мобільному пристрої користувача, що забезпечує антивірусний захист і фільтрацію трафіку.

В Україні BYOD розвивається менш активно, ніж у всьому світі. Причина відставання криється в ментальності керівництва, яке звикло перебувати в офісі і того ж вимагає від своїх підлеглих. Старе загартування далеко не єдина причина: захист BYOD, крім сучасних методів управління, вимагає інвестицій у безпеку, на що малий і середній бізнес реагує неохоче. Деякі компанії практикують тотальну заборону використання мобільних пристроїв. Згідно з проведеними дослідженнями, лідером із впровадження BYOD виступає Китай, найзатятішим противником - Японія.

У невеликих компаніях питання захисту від внутрішніх загроз стоїть гостріше, ніж у середньому та великому бізнесі. Це обумовлено відсутністю IT-відділів, служб безпеки і, як наслідок, призводить до безконтрольності співробітників. Для малого бізнесу існують комплексні рішення, що об'єднують

у собі антивірусні компоненти, фільтрацію контенту і трафіку, а також шифрування необхідних даних. До таких рішень висувається додаткова вимога - простота встановлення та налаштування, для того, щоб з ним міг розібратися просунутий користувач, який відповідає за IT-процеси в маленьких компаніях. Наявність у мережі компанії привілейованих користувачів робить мережу вразливою перед діями своїх же співробітників. Привілейовані користувачі нерідко нехтують політиками безпеки компанії, паролі для облікових записів можуть не змінюватися роками. Ба більше, трапляються ситуації, коли кілька співробітників, які мають адміністративні права, використовують один обліковий запис для внесення змін, у такому разі неможливо встановити особу, яка допустила витік інформації. Для контролю привілейованих користувачів існують спеціальні рішення, наприклад Wallix AdminBastion.

1.2.3 Зовнішні загрози

Сучасне програмне забезпечення практично не має вразливостей. Особливо якщо все правильно налаштувати, а також дотримуватися рекомендацій постачальників програмного забезпечення.

Але це не означає, що ваші дані в цілковитій безпеці. Хакери зараз уже не стільки програмісти, скільки психологи.

Є різні способи поцупити дані, наприклад, обдурити співробітника, підмінивши адресу в електронній пошті і запросивши будь-які дані нібито з поштової скриньки директора. Можна зателефонувати і вимагати терміново скинути фінансовий звіт на будь-яку пошту. Варіантів маса.

Також можна підкупити співробітника, запропонувавши йому гроші. Причина, через яку дані витечуть, не особливо важлива, чи то жадібність, чи то наївність. Але варто відразу зазначити, що людина - головна вразливість будь-якої IT-інфраструктури.

Тож прав доступу до даних, а також можливості редагування варто давати співробітникам рівно стільки, скільки потрібно для виконання обов'язків.

Наприклад, не варто давати звичайній секретарці повний доступ до клієнтської бази або фінансових документів компанії. Звичайний менеджер не повинен мати прав на повне редагування клієнтської бази, а бухгалтерка не повинна мати повний доступ до сервера, на якому розміщені бухгалтерські програми, а тільки до самих програм і рівно в тій мірі, яка потрібна для роботи.

Тож під час проєктування системи інформаційної безпеки варто врахувати людський фактор.

Рисунок 1.10 - Зовнішні чинники ризику

Але навіть це може не врятувати повністю. Наприклад, якщо співробітник когось із постачальників вашого програмного забезпечення раптово зіллє вихідний код ПЗ, то проблеми з'являться і у вас, адже хакери зможуть проаналізувати вихідний код, знайти вразливості, а потім використати їх проти вас.

Але знизивши вплив людського фактора, ви значною мірою збільшите безпеку вашої IT-інфраструктури. Навіть якщо будуть витоки, то не будуть злиті всі дані, тільки частина. Теж неприємно, але не фатально.

Професійні кіберзлочинці діють виключно у фінансових інтересах, винаходячи нові способи проникнення в комп'ютерні системи. Яскравим прикладом шкідливої програми, націленої на крадіжку фінансової інформації, стала троянська програма Zeus. Багатомодульність програми дає їй змогу здійснювати всебічне шпигунство на зараженій машині, відмітною особливістю «Зевса» стало використання мобільної версії, яка відповідає за перехоплення mTAN кодів у SMS від банків. Серед атакованих організацій представлені українські банки і платіжні системи. Малий бізнес через свої особливості менш захищений, ніж середній і великий бізнес. Будь-який системний адміністратор може розповісти безліч історій, як у невеликих організаціях йому доводилося боротися із зараженням і його наслідками. Нерідко в маленьких компаніях користувачі працюють із правами адміністратора. Нічого дивного в цьому немає, але відсутність розуміння необхідності комплексного захисту в таких організаціях грає злий жарт із фінансами компанії. Запобігти зараженню обходиться значно дешевше, ніж нейтралізація та усунення наслідків. На жаль, поки «грім не вдарить» - рідко хто замислюється над цими питаннями.

Популярність спам-атак знижується з кожним роком. Якщо середній бізнес бачить у спамі загрозу, яка може паралізувати обмін інформацією в компанії, то представники малого бізнесу скептично ставляться до цієї проблеми, найчастіше в організації відсутній навіть власний поштовий сервер, співробітники користуються публічними сервісами для обміну інформацією.

У кіберзлочинному світі існує маса угруповань, готових за певну плату здійснити DDoS-атаку на сайт неугодної компанії. Атакований ресурс стає недоступним і компанія - жертва зазнає збитків, пов'язаних із недоступністю сервісів. Збиток від атак має не тільки фінансовий, а й репутаційний характер. Великий бізнес усвідомлює небезпеку DDoS-атак і намагається підготувати та захистити свою інфраструктуру від можливої атаки, проте виходить далеко не

завжди. Ботнети, що використовуються для атак, здатні генерувати трафік у десятки Gb/s, захист у такій ситуації стає нетривіальним завданням.

Фішинг, який зарекомендував себе в злочинних колах, активно набирає обертів і застосовується зловмисниками для отримання конфіденційної інформації. Наприклад, за допомогою фішингової атаки в 2013 році хакер зміг отримати дані 2 млн. абонентів Vodafone Germany. Співробітники компаній стали частіше використовувати мобільні гаджети для роботи і загроза крадіжки девайса, який має доступ до корпоративної мережі, постійно зростає.

1.2.4 Ризики для малих компаній

Ті самі, що й для великих:

- розкрадання даних, зокрема персональних, а також технології, договори, бази клієнтів, інформація про поточні угоди;
- взлом або розкрадання сайту. Може бути дуже чутливо для компаній, які залучають основний потік клієнтів саме через інтернет;
- фішинг, завдяки якому можна отримати доступ до банківського рахунку або корпоративної банківської картки;
- віруси-здирники і шифрувальники, які не тільки вимагають грошей, а й гальмують усі робочі процеси.

Невеликі компанії найбільш схильні до кіберзагроз і з низки внутрішніх причин:

- немає налаштованої системи резервного копіювання та відновлення даних;
- немає системи моніторингу обладнання. Точніше є інвентаризація і всі ноутбуки переписані, на всіх проставлено номер. Але поява нового мережевого пристрою може пройти непоміченою;
- немає системи інвентаризації програмного забезпечення;
- відсутні політики безпеки: будь-який співробітник може поставити будь-яку програму і отримати доступ до будь-яких документів;

- Wi-Fi без пароля;
- поштові сервіси на загальнодоступних ресурсах.

Тому немає нічого дивного, що невеликі компанії стають легкою здобиччю зловмисників. І якщо у великої компанії є ресурси для захисту і відновлення, то невелика або середня організація може зазнати величезних збитків. Часом несумісні з життям компанії.

1.2.5 Методи захисту

Безпека полягає в повному проєктуванні всієї інфраструктури. Це не тільки програмне забезпечення, а й обладнання, і персонал, вище вже йшлося, що головна вразливість - людина. Відповідно, краще буде продумати все на початкових етапах.

Іноді краще заздалегідь звернутися до підрядників, щоб подумали за вас, а потім можна було впроваджувати ще на етапі створення IT-інфраструктури, адже зробити все правильно від самого початку простіше і дешевше, ніж виправляти недоліки потім.

Тож ще на етапі проєкту краще потурбуватися про інформаційну безпеку, чого багато компаній не роблять, бажаючи заощадити або просто не розуміючи ситуацію, а потім серйозно за це розплачуються.

Часто у компаній немає продуманих регламентів роботи з даними, наприклад, не всі розуміють, як зберігати і розміщувати клієнтські бази, в яких містяться персональні дані. А згідно із законами багатьох країн персональні дані не можна зберігати аби як. Вони мають бути надійно захищені, а в разі витоку можна потрапити на штрафи, а також доведеться наймати юристів для судових засідань, якщо витоки спливуть.

Але проблеми можуть бути і з багатьма іншими аспектами, наприклад, хтось може мати доступ до комп'ютера іншого співробітника, хтось може робити скріншоти будь-яких даних і пересилати їх поштою.

Загалом, проблем може бути безліч, і замість того, щоб потім розсьорбувати наслідки, краще заздалегідь скласти політику роботи з даними.

Чіткі регламенти дадуть змогу знизити ризики, і, відповідно, дотримання регламентів буде обов'язком для працівників. Але якщо залишити роботу з даними на відкуп співробітників, то дані не будуть захищені належною мірою.

1.2.6 Рекомендації щодо захисту малих компаній

Є деякі:

- визначити цінність інформації та розподілити її за окремими мережевими папками і налаштувати до них доступ. Чи повинен маркетолог бачити мати доступ до рахунків і договорів? Чи повинні менеджери з продажу мати доступ до всієї звітності? Швидше за все ні;
- налаштувати на кожному робочому пристрої доступ за логіном і складним паролем. В ідеалі паролі треба міняти раз на три місяці;
- провести повну інвентаризацію обладнання. Усе, що викликає підозри, має бути ізольовано і перевірено;
- провести повну інвентаризацію програмного забезпечення. Видалити все, що не стосується конкретних завдань співробітника;
- заборонити співробітникам встановлювати будь-яке програмне забезпечення;
- налаштувати систему подвійного резервного копіювання критично важливих даних: одна копія має зберігатися на фізичному носії в недоступному для співробітників місці, а друга - в захищеній хмарі;
- за можливості заблокуйте користувачам соцмережі та файлообмінні мережі, зокрема хмарні.

Перелік основних рекомендацій:

Антивірус	Швидше за все вже встановлено і головне, щоб він регулярно оновлювався.

Міжмережевий екран	Буває програмним, буває у вигляді окремого пристрою, який фільтрує трафік. Тут підійде Traffic Inspector Next Generation. У нього є версія для малого і середнього бізнесу. Перевіряє трафік, блокує підключення, сайти й окремі протоколи (щоб співробітники не качали торренти). Має власний антивірус, який може додатково посилити можливості встановленого антивіруса раніше.
Додаткова аутентифікація	Перш, ніж увійти в робочий комп'ютер співробітнику треба буде отримати СМС з перевірочним кодом. Особливо актуально для захисту робочих машин бухгалтера, директора або ключових співробітників. Просте рішення є у компанії ESET.
Моніторинг роботи співробітників	Може працювати і як DLP. Програма постійно стежить за пристроями співробітників: сайти, відкриті документи, продуктивність, копіювання файлів. Усе збирається в зручні звіти. Таким чином можна відстежити співробітників, які готові звільнятися. А за ними потрібен особливий контроль.
Комплексні рішення	Шифрування даних і резервне копіювання файлів Захист платежів Захист бізнес-додатків

Таблиця 1.1 - Перелік основних рекомендацій

Звичайно, є й інші продукти для захисту компанії. Адже не буває універсальних рішень, а отже, до кожного завдання потрібно підійти індивідуально.

Провести моніторинг поточних загроз, поставити необхідне ПЗ та обладнання. За необхідності навчити системного адміністратора.

1.2.7 Програмне забезпечення та робота з ним

Програмне забезпечення - вразлива частина. І не тільки через те, що кривими руками код написаний, а й тому, що частенько кривими руками програмне забезпечення налаштоване.

Кожне ПЗ має низку вимог і рекомендацій, які можуть бути несумісними з іншими програмами. Наприклад, для якихось програм потрібно відкрити певні порти на сервері, а також дати численні дозволи. І це не дасть змоги зламати це ПЗ, оскільки воно розраховане на роботу в цих умовах.

Але наявність відкритих портів і певних дозволів, наприклад, для файлової системи, може стати серйозною вразливістю для інших програм. У принципі, це потрібно враховувати ще на етапі проєктування IT-інфраструктури, але світ не стоїть на місці, відповідно, програмне забезпечення оновлюється, з'являються нові вимоги та рекомендації, а це доведеться постійно відслідковувати, щоб у певний момент не створити вразливість власними руками.

Найпоширенішим заходом забезпечення інформаційної безпеки в компаніях залишається використання антивірусного захисту.

Сигнатурних та евристичних методів захисту недостатньо для забезпечення безпеки від новітніх загроз. Для захисту від експлуатування вразливостей в операційній системі та додатках слід використовувати рішення, які містять у собі компоненти аналізу поведінки програм.

Управлінню оновлення програмного забезпечення приділяється велика роль, адже вразливе програмне забезпечення є одним з основних джерел загроз. Для централізованого оновлення розгортаються спеціальні системи, нехтування якими може обернутися мільйонними втратами. Використання мережевих екранів і IDS укупі з DLP дає змогу ефективно протистояти мережевим атакам, вчасно виявляти підозрілий трафік у мережі та виявляти витік конфіденційних даних із компанії.

Більшість компаній розмежовує доступ до IT-систем, відповідно до рівня доступу співробітників підприємства. Вибудовування внутрішньої

інформаційної безпеки без контролю мобільних пристроїв співробітників зводить нанівець заходи щодо запобігання витокам інформації. Мобільні пристрої, будь то смартфони або планшети, можуть бути скомпрометовані зловмисниками для отримання доступу до внутрішньої інфраструктури компанії з її конфіденційною інформацією. Уже зараз існують рішення, що дають змогу забезпечувати комплексний захист мобільних пристроїв, надійно захищаючи їх від шкідливих програм, спаму та фішингу. Мобільний пристрій може бути загублений або вкрадений, в цьому випадку необхідно мати можливість віддаленого контролю пристрою. У разі втрати або крадіжки мобільного пристрою такий функціонал стає незамінним, даючи змогу мінімізувати ризик крадіжки конфіденційних даних.

Визначте, яка саме інформація потребує захисту. Найчастіше доводиться захищати:

- відомості про клієнтів, постачальників, нові розробки та ноу-хау;
- зміст договорів із партнерами;
- собівартість продуктів і послуг;
- аналітичні та маркетингові дослідження, їхні результати та висновки;
- дані про фінансовий стан компанії та про зарплати.

Оцініть реальну вартість вашої інформації. Система захисту інформації не повинна коштувати дорожче, ніж сама інформація. Завдання власника - вивчити список потенційних об'єктів атаки, оцінити ризики та можливі втрати, розрахувати вартість покриття цих ризиків і вже після прийняти рішення, яким чином їх мінімізувати.

З яких рішень з інформаційної безпеки варто починати малому бізнесу? Для будь-якого бізнесу треба починати з оцінки ризиків - простими словами, розуміння того, яка інформація для них найцінніша і хто її може вкрасти.

Якщо це технологічний IT-стартап, то очевидно, що захищати потрібно насамперед розроблювані вихідні коди. Тоді акцент буде на контроль витоків і крадіжку даних співробітниками (DLP).

Якщо ж це невелике підприємство з виробництва масок або стільців, то насамперед слід звернути увагу на працездатність виробничої лінії та управління замовленнями.

Якщо у нас центр юридичних консультацій, то це конфіденційні дані клієнтів.

Якщо ж захищатися буде інтернет-магазин, то для нього головним буде захист сайту - і тут уже насамперед захищаємося антивірусом на хостингу, міжмережевим екраном і навіть Web application firewall не буде зайвим.

У чому кардинальна відмінність у підході до інформаційної безпеки між великим і малим бізнесом? Якщо говорити з погляду теорії, то різниці немає жодної - будь-який бізнес, а точніше його активи (інформаційні або матеріальні) потребують захисту.

І підхід починатиметься з аналізу ризиків:

- виявилення критичних активностей;
- побудування моделі загроз;
- впровадження засобів захисту;
- відбудування процесу забезпечення безпеки.

Але специфіка бізнесу, як завжди, вносить корективи. Якщо великі та середні компанії, як правило, мають у себе цілі підрозділи, що займаються інформаційною безпекою, вивчають загрози, стежать за змінами законодавства, впроваджують найкращі практики для захисту бізнес-процесів, то малі компанії не поспішають витратитися навіть на такі обов'язкові вимоги, як захист персональних даних клієнтів. Воно й зрозуміло - там якщо і є ІТшник, який приходить, то він же і "безпековець", і ризик-менеджер, а ще й адміністратор засобів захисту в одному флаконі. Тому для малого бізнесу підхід, на жаль, дуже простий: «Поки півень не клюне, нам це все байдуже!». Лише після інциденту хтось замислюється, чому ж це трапилося і добре, якщо враховує помилки в наступному бізнесі.

Аутсорсинг інформаційної безпеки актуальний для дрібного бізнесу? ІБ-компанії чи фрілансери? З аутсорсингом безпеки, як і з будь-якою іншою

послугою - треба рахувати, що вигідніше: тримати свого фахівця чи використовувати людину зі сторони. І якщо для великої компанії з великими проєктами, а також постійним супроводом складних систем, однозначно вигідніше (і безпечніше) створити в себе в штаті виділений підрозділ, то в малому бізнесі з погляду операційних витрат тримати свого висококваліфікованого фахівця може бути дорого. Тому аутсорсинг для таких компаній більш звична тема. Однак зазвичай тільки вона впирається не в створення повноцінної системи захисту, а в ІТшні завдання, коли фахівець, що приходить, їм встановить то зламаний антивірус, то допоможе налаштувати піратську версію бухгалтерської програми, то поміняє картриджі в принтері. Ось така безпека. З тієї самої причини, з якої ми розділяємо похід до стоматолога і до лора (у них різна спеціалізація), так і ІТшні завдання (заміна картриджа, протягання мережі, заміна сервера тощо) не повинні плутатися із завданнями ІТшними (захист сервера, контроль співробітників, введення режиму конфіденційності на підприємстві тощо).

Хто це має робити? Очевидно, що це має бути фахівець, який може бути і фрілансером, але найчастіше буде у складі команди в невеликому інтеграторі, що спеціалізується на питаннях інформаційної безпеки, адже «рибалка рибалку бачить здалеку», і той, хто професійно ловить рибу, навряд чи займатиметься ще й пошиттям наволочок на комерційній основі, - тобто суміщатиме розв'язання непрофільних завдань.

Використання хмарних технологій найкращий вихід для невеликого бізнесу для запобігання витокам інформації? Краще розділити: чи потрібно використовувати малим компаніям хмарні технології та наскільки "хмари" безпечні. Хмарні сервіси сьогодні активно розвиваються і нерозумно було б ними не користуватися. Якщо кілька років тому великі компанії (зокрема системні інтегратори) активно будували свої власні центри обробки даних для розміщення серверів, то сьогодні на базі цих потужностей з'явилися і надаються послуги з безпечного зберігання.

Там усі засоби захисту будуть уже встановлені. Чому б ним і не скористатися? Наскільки це безпечно і чи можуть звідти витекти дані? Безпечно, але дані витекти можуть звідки завгодно - навіть з особистого комп'ютера генерального директора. Імовірність того, що вони витечуть зі спеціально створеного сервісу, в якому застосовуються та регулярно оновлюються сучасні засоби захисту, набагато менша, ніж із захищеної лише домашнім маршрутизатором офісної мережі.

Знову ж таки це все прораховується на етапі складання моделі загроз. З огляду на ризики обирають засоби захисту. За грамотного підходу тут не може бути неприємних сюрпризів!

Чи варто відмовлятися від використання open source рішень? Наприклад, розробляти сайти на Bitrix, а не WordPress. Або ж open source рішення теж можна захистити від злому? Насправді не всі комерційні продукти кращі за open source, так само як і справедливо протилежне: коли йдеться про велику любов до open source, то в більшості випадків краще заплатити і купити комерційний продукт, який буде з підтримкою і постійними оновленнями.

Тому і те і те рішення можна захистити, для цього існують і інтегровані, і "навішені" засоби захисту. Головне вміти ними керувати. Краще звісно дотримуватися принципу: «Використовуй те, що краще знаєш». У цьому разі фахівець хоча б має контроль над системою та засобами захисту.

Чи варто стежити за користувачами або потрібно відсіювати потенційно небезпечних користувачів на співбесіді? Знову непросте питання, бо тут теж немає однозначного рішення. «Чи варто стежити за всіма користувачами?». З одного боку, чому б і ні? Вписав відповідний пункт до трудового договору, встановив DLP-систему і «стеж на здоров'я»! Однак, це може також демотивувати співробітників (навіть якщо вони нічого не збиралися вкрасти), вимагає додаткових витрат на придбання і потім на супровід рішень з контролю співробітників. Якщо в компанії в принципі «плинність» і немає злагодженої корпоративної культури, а роботи потрібно виконувати «тут і зараз», то

встановити DLP систему для контролю менеджерів - це рішення, яке очевидно напрошується.

Чи варто при цьому брати всіх підряд і відмовлятися від скринінгу (фільтрації) на співбесіді? Однозначно ні. На співбесіду потрібно запросити профайлера/психолога, який, виходячи з вимог до кандидата, допоможе відфільтрувати або неадекватних особистостей, або тих, хто не схильний до виконання необхідних завдань. Наприклад, «істероїд» або «гіпертим» підійде у відділ маркетингу як креативник, але на роль бухгалтера його категорично не рекомендується брати. А ось «епілептоїд» буде дуже корисний і як кошторисник, і як управлінець середньої ланки. Тоді як «тривожно-недовірливий» чудово згодиться для ризик-аналізу.

Можна резюмувати так: DLP-система однозначно корисна в тих ситуаціях, коли згідно зі складеною моделлю існує високий ризик крадіжки інформації своїми співробітниками. Також для контролю дій співробітників на рівні мережі, коли хочеться закритися від більшості загроз одним засобом за умови обмеження бюджету, рекомендується звернути увагу на рішення класу NGFW - вони покажуть, хто, з якими ресурсами і коли працював.

Від яких каналів і способів передавання даних потрібно відмовлятися бізнесу під час передавання інформації обмеженого доступу? Месенджери? Перед передачею конфіденційної інформації необхідно спочатку визначити, що ж таке конфіденційна інформація - дуже часто в компаніях співробітники просто не розуміють, яку інформацію якими каналами можна передавати. Але це доти, доки не створено чіткий регламент і політики обробки конфіденційної інформації. У них і прописується, виходячи з ризиків для бізнесу, що можна використовувати, а від чого слід утриматися. Якщо говорити більш конкретними, але при цьому універсальними рекомендаціями, то необхідно заборонити передачу конфіденційної інформації через месенджери та соціальні мережі. Є перевірені та зрозумілі канали: електронна пошта, яку можна зашифрувати та захистити від перехоплення, електронний документообіг, який

компанії можуть сьогодні здійснювати навіть за допомогою хмарних сервісів, передаючи одна одній просто посилання на документи.

Якщо у компанії якась розробка застосунків або сервісів, то тоді взагалі немає сенсу кудись передавати інформацію, окрім ситуацій, коли застосунки та сервіси публікують для користувачів, і тут вони, за визначенням, мають бути доступними. Передача вихідних кодів для перевірок або сертифікації здійснюється offline методом на відчужуваних носіях (USB або CDROM). А якщо є така можливість, то взагалі краще надати можливість перевірки процесу складання вихідних кодів прямо на майданчику компанії, організувавши контроль доступу до цих ресурсів.

Загалом, для кожної компанії треба розбиратися, навіщо їй взагалі кудись передавати свою конфіденційну інформацію. І в будь-якому разі слід використовувати захищені від перехоплення та підміни канали зв'язку (наприклад, VPN по відкритих каналах зв'язку між підрозділами та офісами), і не використовувати засоби особистої комунікації (наприклад, згадані месенджери) для обміну конфіденційною інформацією.

Як правильно вибудувати процес підвищення обізнаності користувачів? Це наступне логічне завдання після запровадження режиму конфіденційності в організації. Процес обізнаності має важливі властивості: він має бути. він має бути регулярним.

Співробітники в 99% - це користувачі, які не є фахівцями в галузі захисту інформації, тому не можна покладатися ні на їхні знання, ні на відповідальність - наприклад, що вони захочуть зануритися в деталі інформаційної безпеки. Для них необхідно випускати чіткі інструкції простою «призначеною для користувача» мовою і проводити «тренінги обізнаності» - корпоративні навчання, коли робиться спеціальна перевірочна фішингова розсилка без повідомлення користувачів з дозволу генерального директора і потім оприлюднюються результати і робляться висновки. Або ж проводяться щомісячні лекції та міні-тренінги від відділу захисту інформації або залученими фахівцями, де розповідають останні новини зі світу безпеки,

роз'яснюють необхідність використання засобів захисту, проводять навчання їх застосування.

Зараз у деяких компаній з'явився формат віддалених курсів підвищення обізнаності користувачів з можливістю навіть атестації та проведення «корпоративних навчань» і все це онлайн.

Чи можливо розробникам прищепити культуру безпечної розробки? Що робити якщо немає грошей на дорогі сканери вихідного коду? Розробникам треба задавати правила розробки в компанії, яких вони дотримуватимуться. Це як обрана нотація чи формат розробки - встановлена на рівні компанії і всі мають її дотримуватися. Тому і сценарії безпечної розробки мають бути встановлені як стандарт у компанії. Після цього і сканери вихідного коду, можливо, і не потрібно буде застосовувати. Вірніше їх можна використовувати не постійно, а як разову послугу під час випуску важливого релізу. Так роблять багато компаній.

Але тут важливо розуміти, що якщо впроваджено стандарти безпечної розробки (SecDevOps), то ще до етапу застосування сканерів безпеки можна уникнути багатьох проблем. Грамотне проєктування, прототипування (наприклад, мікросервісна архітектура з принципами «нульової довіри» між модулями), супровід розроблення і взаємодія між командами ІБ та ІТ, впровадження методик автоматичного тестування...

Зрештою, можна впровадити засоби захисту - наприклад, WAF для веб-сервісу, який дасть змогу знизити ризик компрометації застосунку через потенційну вразливість навіть за відсутності сканерів безпеки.

Чи правильно, що найвразливіші місця в будь-якій компанії - це користувачі? Дуже часто користувачі, дійсно, виявляються слабкою ланкою в системі захисту. Можна скільки завгодно захищати периметр і фільтрувати вхідну пошту на предмет наявності вірусів, але працівник може принести щось всередину периметра на своєму особистому ноутбуці або флешці (якщо їхнє використання мається на увазі в компанії, а тому їх не можна заблокувати засобами захисту на робочих місцях, - хоча й у цьому разі є рішення,

наприклад, дозволити тільки певні типи флеш-накопичувачів, хоча й це не позбавить вірусів на дозволених флешках, зате звузить площу атаки).

У будь-якому разі внутрішній співробітник може бути й інсайдером, тому також слід розглянути використання засобів моніторингу поведінки (UEBA), контролю витоків (DLP), а також у будь-якому разі не забувати про власне захист робочих місць (EPP, EDR), щоб потенційна загроза не могла заразити комп'ютер співробітника, який зазівався.

Також із цієї причини важливо запроваджувати або свій власний університет корпоративного навчання в галузі безпеки - підвищення обізнаності, або подумати над аутсорсингом цієї послуги.

Чи правильно, що найкращий захист від усіх атак - це резервне копіювання? Давайте розглянемо на такому прикладі. Припустимо, у компанії впроваджено резервне копіювання для цілісності та доступності бази даних клієнтів, визначено показники RTO, RDO. А що буде, якщо в резервну копію потрапить вірус? А як дізнатися, яка саме резервна копія не заражена? А якщо перезаписано останню незаражену стару версію даних новою, але в яких є вірус. Як отримати про це хоча б попередження?

Бачимо, що тільки резервним копіюванням тут не обійтися. Ідеально поєднати резервне копіювання з антивірусним захистом, а також із "пісочницями" - це коли файли не тільки перевіряються за сигнатурами, а ще й за поведінкою. У цьому разі «пісочниця» (sandbox) перекладає перевірені чисті файли до спеціального каталогу, який уже, своєю чергою, і підлягає резервному копіюванню.

Чи правильно, що розмір фінансів, витрачених на ІБ, не повинен перевищувати вартість захищеної інформації? Це твердження справедливе і логічне. Настільки логічно, що ні в кого не виникає запитань.

Однак для бізнесу є інша проблема, з цим пов'язана: «А як оцінити вартість захищеної інформації або ресурсу?». Зазвичай для цього застосовується експертна оцінка. Але це суб'єктивний фактор.

Також під час розрахунку ризиків враховується не тільки цінність активу, а й імовірність реалізації загрози, яку теж непросто поміряти. Зазвичай тут також покладаються на накопичену статистику або експертну оцінку.

Але всі усвідомлюють, що малий бізнес витрачати мільйони доларів на створення системи безпеки не буде - адже часто це навіть більше за оцінку самого бізнесу.

У будь-якому разі бізнес узагалі має розуміти, навіщо йому, наприклад, дорогий міжмережевий екран, якщо в них сайт не основний канал продажів, або навіщо міняти антивірус на новіший, якщо наявний з усім справляється, а новий у впровадженні та подальшому супроводі дорожчий за старий.

Щодня з'являються нові вразливості. Чи означає це, що потрібно щодня ставити патчі, встановлювати нові версії ПЗ, щоб уникнути витоку інформації? В ідеальному світі картина має саме такий вигляд: виходить вразливість – з’являється патч, одразу ж усі системи самі оновлюються і виявляються захищеними.

У реальному житті великих компаній і складних систем із багатьма залежностями та великою відповідальністю перед клієнтами все складніше: вони не можуть ризикнути і встановити патч, який обов'язково змінить якісь налаштування і заздалегідь незрозуміло, як це відіб'ється на інших пов'язаних модулях і системах.

Тому обов'язково використовують тестове середовище: системи, які дублюють у зменшеному масштабі основний контур і на яких розгортаються патчі, щоб переконатися, що після оновлення система продовжить працювати без збоїв.

При цьому для нівелювання ризику під час вікна вразливості, коли патчі ще не встановлені, а загроза існує, є кілька способів:

- застосування технології «віртуального патча» - це або мережева, або вузлова система захисту, яка детектує і блокує спроби експлуатації вразливостей;

- прийняття ризику власником бізнес-системи або процесу на себе, якщо немає можливості купити і встановити або налаштувати засоби захисту під знову виявлені загрози.

Для малих компаній, про які ми і ведемо мову тут, все простіше - тут, як правило, немає складних систем, залежностей модулів, але також і немає можливості витрачати і без того обмежені ресурси на створення пілотної зони. А ще немає грошей на ефективні в таких ситуаціях системи «віртуального патча». Власники воліють брати ризики на себе в надії, що їхню компанію ніхто не зламає.

Тому для цих компаній загальна рекомендація - ставити патчі якомога швидше, коли вони з'являються. А також використовувати хоча б один універсальний засіб - наприклад, уже згаданий NGFW - комбінований пристрій, який вирішує одразу кілька завдань захисту компанії за принципом «комбайна».

Яке майбутнє чекає на компанії, що надають послуги з ІБ? Чи варто чекати, що незабаром усе більше клієнтів купуватиме не СЗІ, а сервіс із захисту даних? Для середніх і малих компаній можливість заощадити на капітальних витратах і розбити платежі, перенісши їх в операційний бюджет, - це прямо як ковток повітря. Та й для сервісних компаній це зручніше - стабільний і передбачуваний грошовий потік.

Тому за сервісною моделлю майбутнє.

Давайте подивимося на великі компанії, які також винесли багато напрямків, зокрема захист інформації в окремі юридичні особи. Вони, як правило, надають послуги тільки для своєї материнської компанії. Через кілька років успішної роботи, щоправда, такі сервісні компанії можуть розвиватися і брати на обслуговування інші схожі організації.

Але це абсолютно не скасовує необхідності купівлі та встановлення засобів захисту. Адже сервісна компанія налаштовує, оновлює, стежить за працездатністю тільки того, що існує. Як варіант економії знову ж таки можна розглянути варіант «оренди засобу захисту» - ось цих послуг поки що на ринку

справді небагато і за ними майбутнє - повністю сервісна модель як для послуг, так і для обладнання.

1.2.8 Топ 5 рішень (класів рішень) для малого бізнесу

За зменшенням популярності:

- антивірусні засоби;

  Для Українського бізнесу пропонують наступні антивірусні засоби:

  1. Укртелеком пропонує рішення ESET для захисту корпоративної IT-інфраструктури

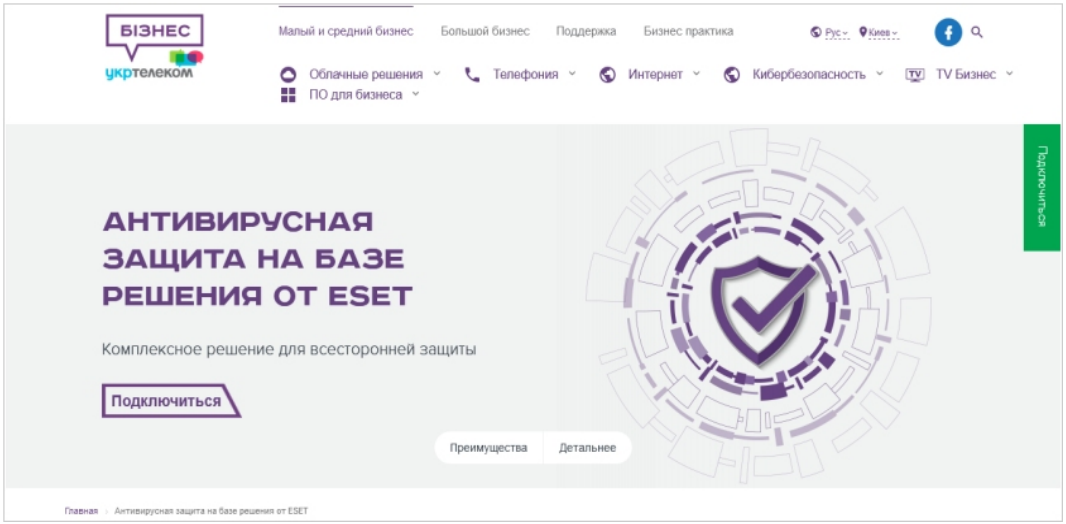


Рисунок 1.11 - Сайт Укртелеком Бізнес

Укртелеком розширює власний асортимент інструментів для забезпечення захисту IT-інфраструктури за рахунок продуктів словацького вендора ESET. Антивірусний захист від ESET – послуга, що запобігає кібератакам і надає комплексний захист фізичних та віртуальних робочих станцій, серверів та мобільних пристроїв.

  2. Bitdefender пропонує безкоштовну допомогу з кібербезпеки українським компаніям

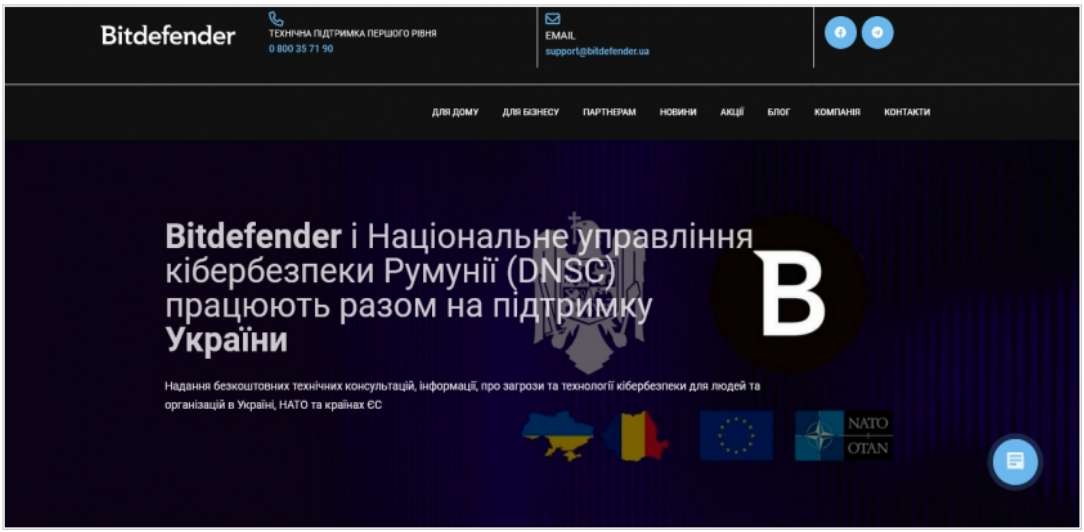


Рисунок 1.12 - Сайт антивірусу Bitdefender

Румунський розробник антивірусного програмного забезпечення та систем кібербезпеки Bitdefender пропонує надання технічних консультацій, розвідки загроз та технологій кібербезпеки для українських громадян та організацій. Лабораторії Bitdefender з дослідження кіберзагроз та Центр операцій з безпеки постійно відстежують кібератаки, спрямовані на простір НАТО/ЄС, та випускають попередження про нові результати.

3. Microsoft Defender for Business

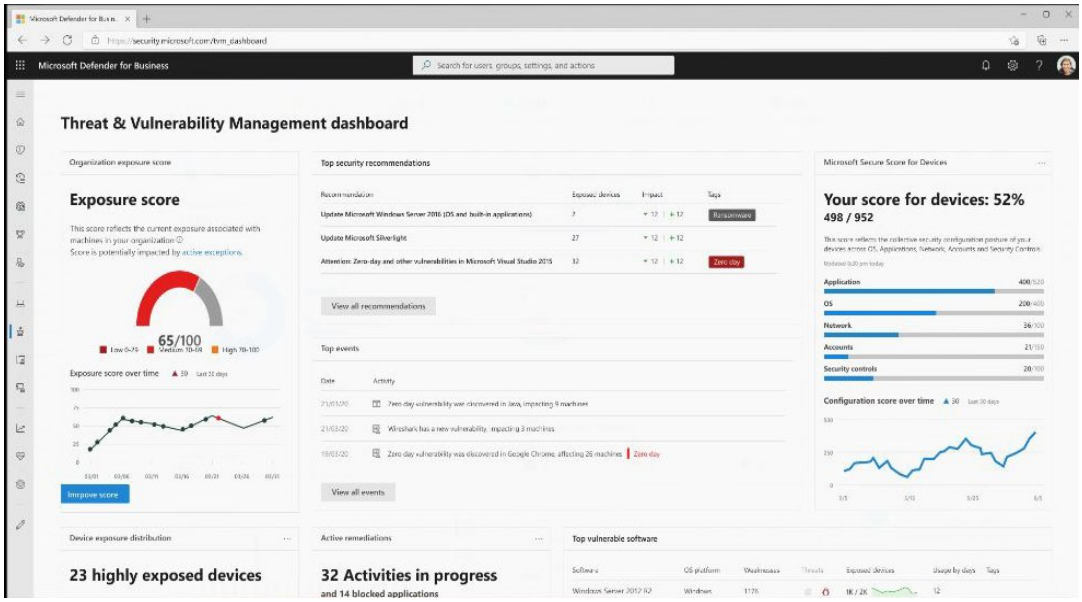


Рисунок 1.13 - Сайт Microsoft Defender for Business

Хоча антивірус Microsoft Defender доступний безкоштовно у складі Windows, його можливостей не завжди вистачає щоб надійно захистити офісну мережу в компанії. Спеціально для малого середнього бізнесу (компаній чисельністю до 300 співробітників) Microsoft випустила бізнес-версію антивірусу.

4. Zillya! Антивірус – український антивірус для бізнесу

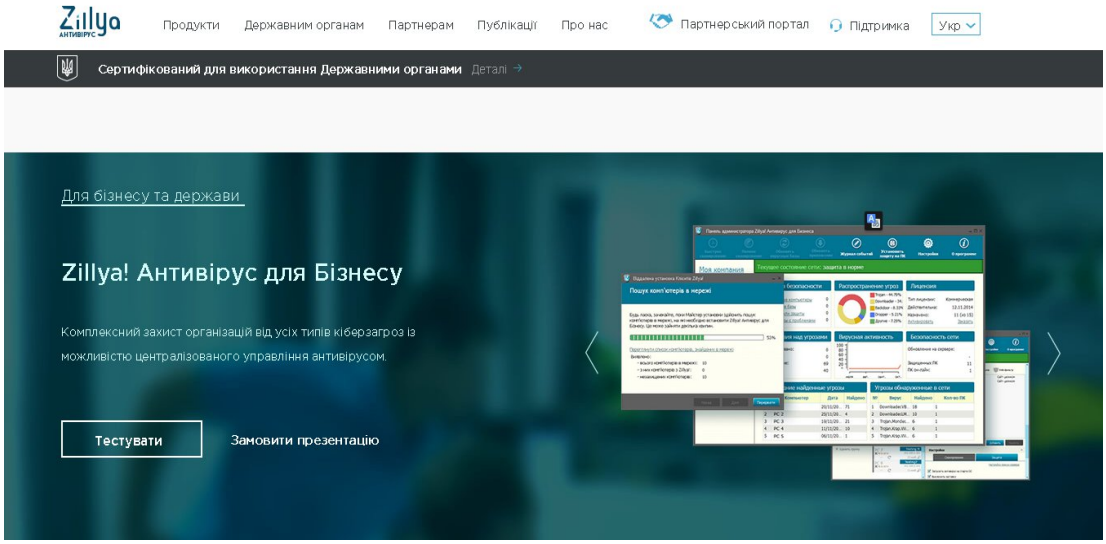


Рисунок 1.14 - Сайт Zillya! Антивірус

Zillya! Антивірус для бізнесу - сучасне рішення, створене для формування надійного кіберзахисту корпоративних клієнтів. Відмінною особливістю даного продукту є формат комплексного захисту організації від всіх типів кіберзагроз з можливістю централізованого управління антивірусом.

- міжмережеві екрани (в їхніх різновидах);

Міжмережеві екрани – це захисне обладнання, націлене завдання контролю мережі (домашньої чи корпоративної) щодо цифрових загроз через вхідний трафік.

Рисунок 1.15 - Fortinet Fortigate Fg-60f 10 Брандмауер порту Rj 45

Що забезпечує мережевий екран? Файрвол блокує спроби зовнішнього несанкціонованого доступу до мережі, закриваючи вразливості цифрових протоколах чи ОС кінцевої точки (сервер, ПК).

Генеральний функціонал для Firewall

Щоб купити міжмережевий екран, необхідно позначити сферу завдань, що вирішуються пристроєм.

Стандартний фаєрвол найбільш затребуваних виробників і марок, як правило, виконує функції:

- ідентифікація та контроль софту кінцевих точок, що діють певні порти;
- шифрування та дешифрування мережевого трафіку в обох напрямках;
- інспекція невідомого трафіку;
- скан портів щодо наявності шкідливих програмних кодів;
- менеджмент активних аплікацій;
- оптимізація швидкості роботи системи та вузла за умов функціонування сек`юрного блоку;
- пошук та відстеження випадків вторгнення до захисної системи.

З метою розуміння відповідності обраного пристрою запитам конкретного споживача пропонується типова опціональна класифікація, за якою підбираються міжсетеві апаратні екрани.

Фаєрвол: поділ за типами

Брандмауер, головним чином, розмежовують за своїм форм-фактором, який може бути фізичним чи цифровим.

Програмний мережевий екран - це софт, що інсталюється на кінцеву точку з метою нівелювання спроб несанкціонованого проникнення, небезпечного програмного забезпечення тощо. Як приклад для цього типу можна позначити базовий брандмауер Windows та аналогічні.

Апаратні міжмережові екрани - це пристрої, які виконують завдання програмного екрану, маючи при цьому матеріальну основу.

Не складно здогадатися, що диференціація між програмними/апаратними фаєрволами полягає в тому, що в першому випадку установку потрібно зробити на кожну кінцеву точку, а в другому випадку захист охоплює всю мережу. Звичайно ж, допустимо задіяти апаратний захисник на кожну кінцеву точку, але цей варіант не практикується через свою дорожнечу та трудомісткість процесу.

- антиспам;

Антиспам - це модуль програмного забезпечення, який запобігає та блокує небажані електронні листи, такі як спам.

Антиспам використовує різні засоби для фільтрування небажаних повідомлень, наприклад «білі» та «чорні» списки, списки адрес, авторитетні пошти та відповідні ключові слова. Спам-фільтр присвоює оцінку кожному просканованому повідомленню електронної пошти та використовує цей показник, щоб визначити доставляти повідомлення чи додати його до небажаної пошти.

Верховна Рада України прийняла Закон № 3014 «Про електронні комунікації», проект якого був представлений ще в лютому 2020. І ось на початку 2021 року цей закон був підписаний президентом. Потреба законодавчо впорядкувати сферу електронних комунікацій у нашій

країні назріла давно. Продиктована вона не лише застарілими і суперечливими законами в сфері електронних комунікацій, але й вимогою привести законодавчу базу у відповідність до нормативів, які діють в Європейському Союзі, в межах Угоди про асоціацію між Україною та ЄС. Він набув чинності з 1 січня 2022 року.

У законі йдеться про зменшення кількості перевірок та регуляторного тиску на компанії у сфері електронних комунікацій, а також, що особливо цікавить нас як емейл-маркетологів, про заборону масових електронних розсилок без дозволу одержувачів. Здавалося б, ініціатива логічна і корисна для ринку. Але в цій діжці меду є ложка дьогтю – під визначення «Спам» може потрапити більшість відправлених сьогодні проморозсилок.

Закон дає чітке визначення спаму, що виключає подальшу плутанину з термінологією.

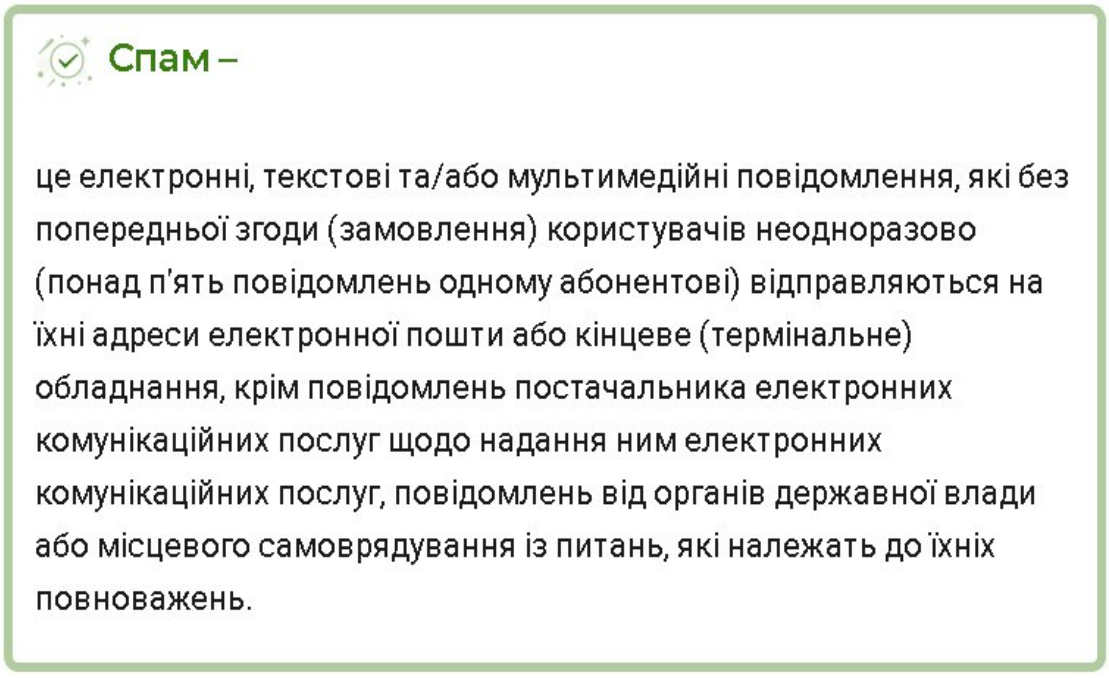


Рисунок 1.16 - Чітке визначення слову спам

Забороняються неодноразові відправлення електронних листів, мультимедійних та текстових повідомлень комерційного характеру без попередньої згоди респондента.

- веб-фільтрація;

Веб-фільтрація, або інтернет-фільтр - це програмний або апаратний засіб для забезпечення фільтрації веб-сторінок за їхнім вмістом, що дає змогу обмежити доступ користувачам до певного списку сайтів або послуг в інтернеті.

Системи веб-фільтрації можуть бути виконані в різних варіаціях:

- утиліти;
- додатки;
- доповнення для браузера;
- доповнення для інтернет-шлюзів;
- хмарні сервіси.

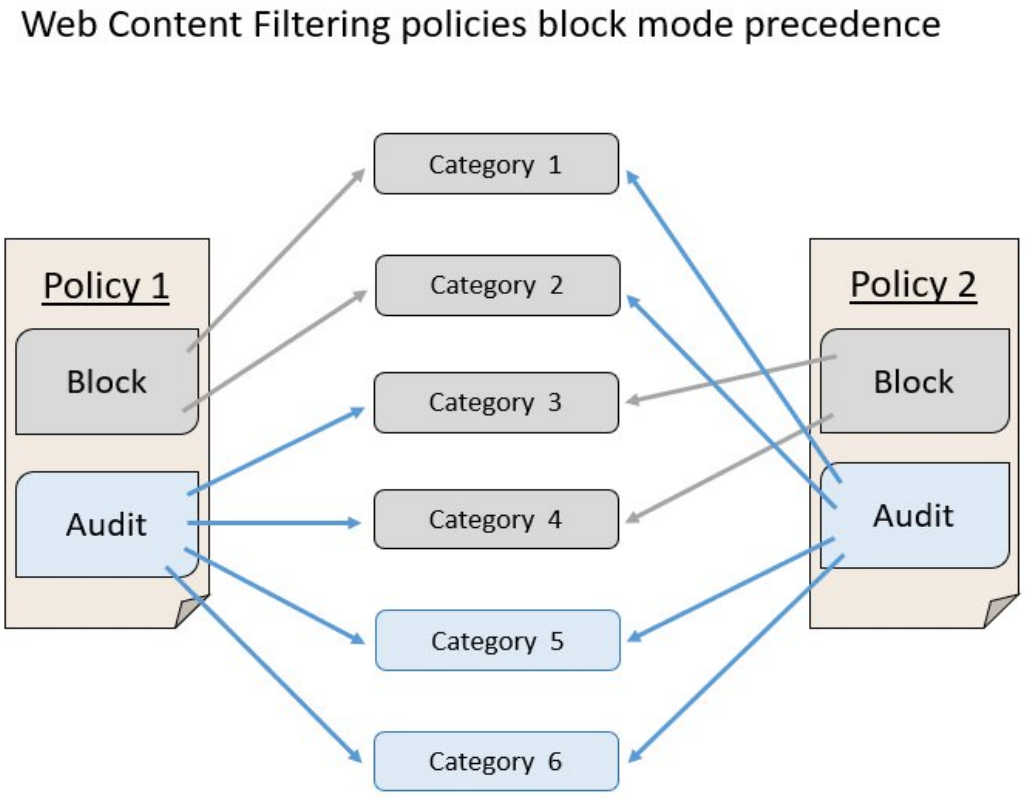


Рисунок 1.17 - Політики фільтрації веб-вмісту блокують режим точності

Засоби веб-фільтрації запобігають відвідуванню небезпечних сайтів, на яких розміщено шкідливі програми або які віднесено до

числа фішингових сайтів. Але головним їхнім завданням є управління доступом до веб-сайтів певних категорій. З їхньою допомогою можна легко обмежити співробітникам компаній доступ до всіх веб-сайтів певних категорій.

Весь вхідний трафік аналізується і розподіляється за категоріями. Залежно від налаштувань засобу інтернет-фільтрації може бути заблоковано доступ до певної категорії контенту, а користувачеві на екран буде виведено попередження.

- контроль співробітників (наприклад, DLP).

DLP-система (Data Loss Prevention) — це програмний продукт, створений для запобігання витоку конфіденційної інформації за межі корпоративної мережі. Будується ця система на аналізі потоків даних, що виходять за межі корпоративної мережі. У разі спрацювання певної сигнатури та детекту передачі конфіденційної інформації система або блокує таку передачу, або надсилає повідомлення офіцеру безпеки.

Після впровадження системи захисту даних від витоку компанія отримає:

- захист інформаційних активів та важливої стратегічної інформації компанії;
- структуровані та систематизовані дані в організації;
- прозорості бізнесу та бізнес-процесів для керівництва та служб безпеки;
- контролює процеси передачі конфіденційних даних у компанії;
- зниження ризиків пов'язаних із втратою, крадіжкою та знищенням важливої інформації;
- захист від шкідливого ПЗ, що потрапляє в організацію зсередини;
- збереження та архівація всіх дій пов'язаних із переміщенням даних всередині інформаційної системи.

2 ОХОРОНА ПРАЦІ

Охорона праці - це сукупність заходів, які спрямовані на запобігання травматизму та захист здоров'я працівників на робочому місці. Кожен працівник має право на безпечні та здорові умови праці, але це не завжди можливо без виконання певних норм та правил. З метою забезпечення безпеки та охорони здоров'я працівників багато країн світу створюють законодавчу базу, яка регулює питання охорони праці на різних видовищах.

Для поліпшення умов і охорони праці необхідна ефективна співпраця між всіма рівнями державної влади та громадськості, а також реалізація програм на державному та місцевому рівнях. Реалізація цих програм може допомогти розробити систему нагляду, навчання та контролю в галузі охорони праці, адаптувати законодавство до європейських стандартів, забезпечити інформаційне та науково-методичне забезпечення і створити безпечні умови праці на підприємствах та в організаціях усіх форм власності. Все це допоможе забезпечити пріоритет життя та здоров'я працюючих та забезпечити комплексне вирішення задач охорони праці.

У світі існують різні види професій та виробництв, де вимагається дотримання особливих правил та норм, щоб забезпечити безпеку працівників. Охорона праці стала невід'ємною складовою в будь-якій сфері діяльності, де є люди. Вона дає можливість не тільки забезпечити безпеку працівників, але й ефективно вирішувати проблеми на робочому місці та знижувати ризик виникнення небезпечних ситуацій.

2.1 Аналіз та безпека умов праці працівника на робочому місці

2.1.1 Організація робочого місця

Шкідливі фактори, пов'язані з використанням комп'ютерної техніки, можуть мати негативний вплив на здоров'я користувачів. Ці фактори включають неправильну поставу, напругу очей, шум, електромагнітне

випромінювання, біологічні фактори та дезорганізацію режиму роботи та відпочинку.

Неправильна постава може призвести до болей у спині, шиї, руках та зап'ястях. Розглядання екрану комп'ютера може призвести до напруження очей, що може спричинити головні болі, сухість очей та інші проблеми зі здоров'ям очей. Комп'ютери можуть видавати шум, що може викликати стрес та зниження працездатності.

Електромагнітне випромінювання може мати шкідливий вплив на здоров'я людини. Клавіатури та миші комп'ютерів можуть бути джерелом мікробів та інших патогенних організмів. Працюючи за комп'ютером, людина може забути про перерви для відпочинку, що може призвести до зниження працездатності та збільшення ризику розвитку хронічних захворювань.

Для забезпечення комфортної та безпечної праці з ВДТ, необхідно застосовувати відповідну організацію робочого місця та обладнання. Всі елементи робочого місця та їх взаємне розташування повинні відповідати ергономічним вимогам, які враховують характер і особливості трудової діяльності (згідно з ГОСТ 12.2.032-78, ГОСТ 22.269-76, ГОСТ 21.889-76).

Робочі місця з ВДТ краще розташовувати так, щоб природне світло падало збоку, переважно зліва. Для робочих столів з ВДТ слід дотримуватися відстаней: між бічними поверхнями ВДТ - 1,2 м; від тильної поверхні одного ВДТ до екрану іншого - 2,5 м. Екран ВДТ має бути розміщений на оптимальній відстані від очей користувача, що становить 600-700 мм, але не ближче, ніж за 600 мм з урахуванням розміру літерно-цифрових знаків і символів.

Клавіатуру слід розташовувати на поверхні столу на відстані 100-300 мм від краю, зверненого до працюючого. Конструкція клавіатури повинна передбачати опорний пристрій, який дає змогу змінювати кут нахилу поверхні клавіатури у межах 5-150.

При обладнанні робочого місця лазерним принтером необхідно враховувати вимоги СанПіН № 5804-91 щодо параметрів лазерного випромінювання.

2.1.2 Вимоги безпеки до мікроклімату, освітлення, шуму ,виробничих випромінювань

Основними документами, які визначають параметри мікроклімату виробничих приміщень, є ДСН 3.3.6.042-99 та ГОСТ 12.1.005-88. Ці параметри регулюються для робочої зони - визначеного простору, де знаходяться робочі місця. Згідно з нормативним документом ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень», параметри мікроклімату мають відповідати значенням, зазначеним у табл 2.1.

Таблиця. 2.1

Параметри мікроклімату приміщення

Період року	Категорія робіт	Температура, С		Відносна вологість, %
		оптимальна	допустима	
Холодний	Легка – Іа	22-24	21-25	40-60
Теплий	Легка – Іа	23-25	22-26	40-60

Приміщення, в яких встановлені персональні комп’ютери, повинні мати природне та штучне освітлення. Природне освітлення здійснюється через світові прорізи (вікна), орієнтовані переважно на північ чи північний схід. Штучне освітлення в приміщені здійснюється системою загального рівномірного освітлення. На поверхні столу в зоні розміщення документів штучне освітлення має становити 300-500лк.

Так як шум має 35Дб, сприйняття шуму людським вухом межується від 20Дб до 120 дб, це означає, що при роботі за ЕОМ шум не заважає, працівнику працювати.

Для запобігання виникнення інших шумів у відповідності з ГОСТ 12.1.029- 80 зниження шуму й вібрації в приміщенні дипломним проектом передбаченні звукоізоляція вікон та дверей.

Для того, щоб забезпечити здорову роботу та запобігти швидкій втомлюваності очей, професійним захворюванням, нещасним випадкам і

підвищити продуктивність праці та якість продукції, необхідно відповідно установити виробниче освітлення.

Конкретно, воно повинно створювати достатню освітленість на робочій поверхні, що буде відповідати характеру зорової роботи та встановленим нормам.

Також важливо забезпечити рівномірність та постійність рівня освітленості у всіх виробничих приміщеннях. Це допоможе уникнути частого переадаптування органів зору та зменшить ризик появи засліплювальної дії. Додатково, на робочій поверхні не повинно бути ніяких різних тіней, а також має бути достатньо контрасту між освітлюваними поверхнями. Також важливо уникати небезпечних та шкідливих виробничих чинників, таких як шум, теплове випромінювання, електрична небезпека, пожежо- та вибухонебезпека світильників.

Нарешті, виробниче освітлення має бути надійним, простим у експлуатації, економічним та естетичним.

2.2 Пожежна безпека

Під поняттям пожежна безпека розуміють систему заходів, які спрямовані на захист людей та майна від вогню. У разі приміщень з електричними мережами, дотримання пожежної безпеки регулюється стандартами ГОСТ 12.1.033-81 та ГОСТ 12.1.004-85. Крім того, для роботи оператора ЕОМ необхідно мати приміщення, яке відповідає категорії Д пожежної безпеки, тобто містить негорючі речовини та матеріали в холодному стані.

До засобів пожежогасіння належать внутрішні пожежні водопроводи (крани - ПК), вогнегасники (вуглекислотні та порошкові), сухий пісок та інші. У будівлях пожежні крани зазвичай розміщують у коридорах та на майданчиках сходових кліток. Кожен пожежний кран обладнаний пожежним рукавом, який знаходиться в спеціальному ящику на висоті 1,35 м від полу.

Для загасання пожеж на початкових етапах широко використовують вогнегасники. У виробничих приміщеннях основною формою вогнегасників є вуглекислотні, які мають високу ефективність у гасінні пожеж, а також дозволяють зберегти електричне обладнання. Вогнегасники розміщують на видному місці на висоті не більше 1,5 м від полу.

Для вирішення евакуаційних задач у виробничих приміщеннях зазвичай є запасні виходи. Двері, які ведуть до запасних виходів, повинні мати освітлений напис «Запасний вихід». План евакуації вивішують на видному місці біля основного виходу. Приміщення, в яких встановлені персональні комп'ютери, повинні мати природне та штучне освітлення. Природне освітлення здійснюється через світові прорізи (вікна), орієнтовані переважно на північ чи північний схід. Штучне освітлення в приміщені здійснюється системою загального рівномірного освітлення. На поверхні столу в зоні розміщення документів штучне освітлення має становити 300-500лк.

У разі виникнення пожежі потрібно зупинити електропостачання, негайно повідомити за номером 101 професійну пожежну команду, дотримуючись плану евакуації, евакувати людей з будівлі і розпочати процедуру гасіння пожежі.

ВИСНОВКИ

Більшість компаній недооцінює ризики пов'язані з кіберзагрозами. Компанії повинні інвестувати в навчання співробітників, пояснюючи базові правила безпечної роботи в мережі та підвищуючи рівень обізнаності про нові загрози. Грамотні користувачі на робочих місцях - хороша основа для інформаційної системи безпеки компанії. Концепція BYOD, що набирає популярності, створює для бізнесу додаткові ризики інформаційної безпеки, для вирішення яких необхідне використання спеціальних політик для мобільних пристроїв і MDM. Питання інформаційної безпеки для невеликих компаній відходять на задній план або взагалі не вирішуються. Співробітники компаній мають права адміністратора, повний доступ до всіх пристроїв і систем, що спричиняє безконтрольне використання ресурсів організації. Окремий захист потрібен під час роботи з системами онлайн-банкінгу та іншими платіжними системами, що дасть змогу убезпечити співробітників від введення даних на фішингових сайтах і перехоплення параметрів доступу до рахунків шкідливими програмами. Невеликим компаніям потрібне універсальне рішення за розумну вартість, що вирізняється простотою встановлення та управління, яке дасть змогу гнучко налаштувати використання ресурсів компанії, а також забезпечить комплексний захист від усіх типів загроз.

Головне правило: безпека має бути комплексною і безперервною, включати моніторинг, заходи захисту і роботу з персоналом. Якщо відмовитися від помилкового почуття безпеки, погляд на управління компанією стає більш тверезим. А управління - розумним.

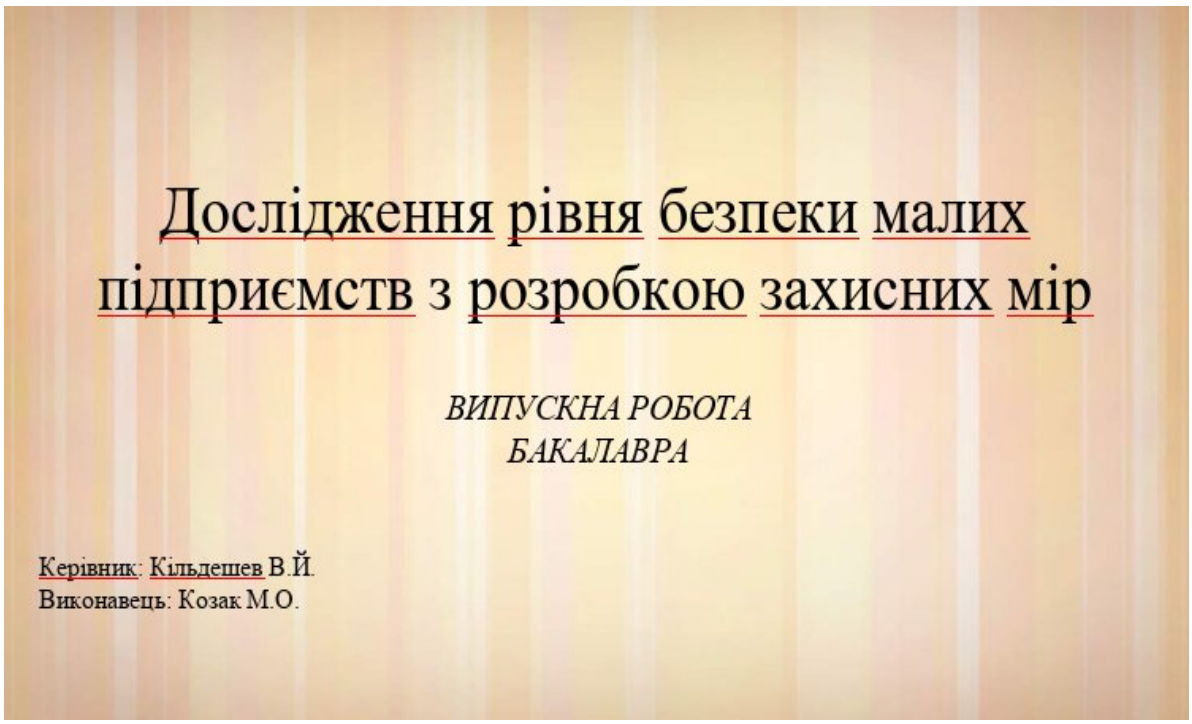
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

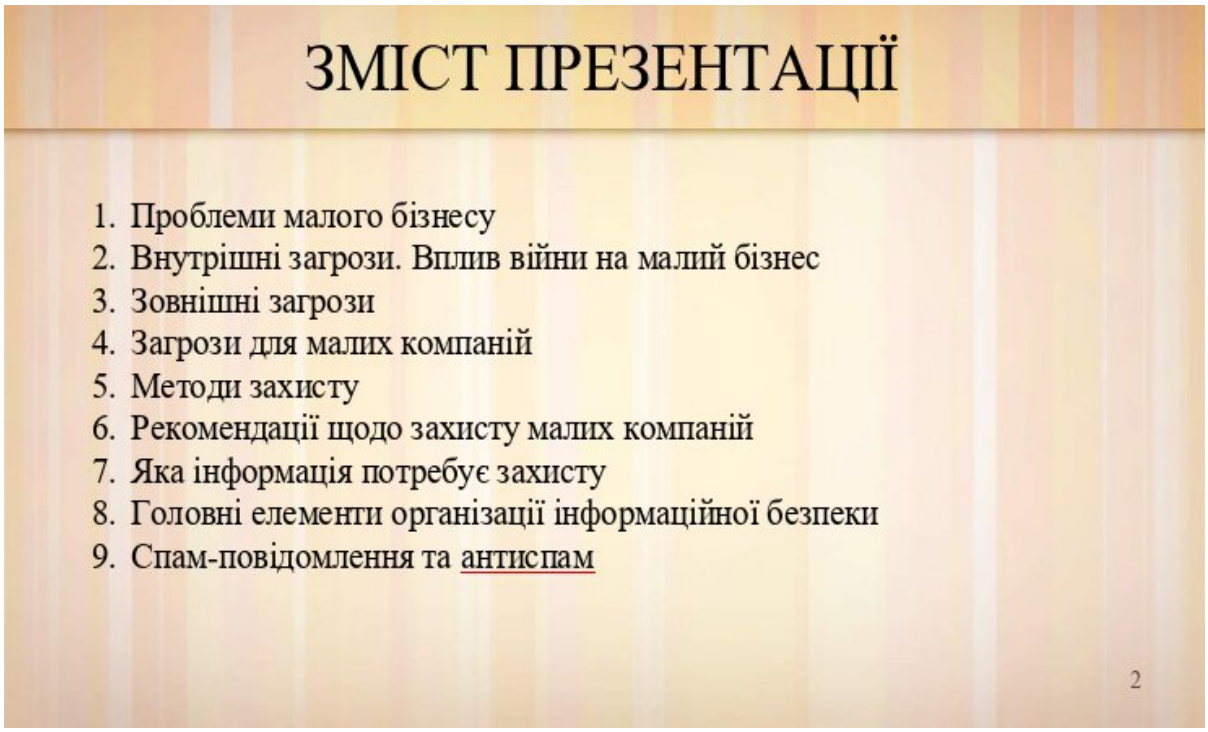
1. О.О. Сосновська. Система економічної безпеки підприємств зв'язку [Електронний ресурс] URL: https://core.ac.uk/download/pdf/241043898.pdf
2. М.В. Міненко. Сутність та види суб'єктів забезпечення економічної безпеки підприємств [Електронний ресурс] URL: http://www.economy.nayka.com.ua/?op=1&z=2802
3. Г. В.Ситник, Г.В. Блакита, Н.М. Гуляєва. Економічна безпека підприємництва в Україні [Електронний ресурс] URL:https://knute.edu.ua/file/MjkwMjQ=/5a209ea36441d3c8a61de7c747ac385b.pdf
4. Загальні положення і класифікація засобів забезпечення безпеки підприємства [Електронний ресурс] URL: https://referatss.com.ua/work/zagalni-polozhennja-i-klasifikacija-zasobiv-zabezpechennja-bezpeki-pidpriiemstva/
5. Ортинський В.Л., Керницький І.С., Живко З.Б., Керницька М.І., Гук О.В., Шимечко Г.І., Живко М.О. Економічна безпека підприємств [Електронний ресурс] URL:https://dspace.lvduvs.edu.ua/bitstream/1234567890/673/1/економічна безпека підприємств підручник.pdf
6. Мельник С.І. Управління фінансовою безпекою підприємств: теорія, методологія, практика [Електронний ресурс] URL:https://dspace.lvduvs.edu.ua/bitstream/1234567890/3284/1/Mel'nyk_монографія.pdf
7. Пташенко Л.О. Стратегічне та інноваційне забезпечення розвитку системи економічної безпеки підприємства [Електронний ресурс] URL: http://reposit.nupp.edu.ua/bitstream/PoltNTU/3087/1/СІЗРСБП Пташенко.pdf

8. Буркан Є.А. Оцінка рівня фінансово-економічної безпеки підприємства [Електронний ресурс]
URL: https://openarchive.nure.ua/server/api/core/bitstreams/489fd52f-2637-4dd4-8c8a-7ed42d443592/content
9. Парфентій Л.А. Управління фінансовою безпекою підприємств в умовах економічної нестабільності [Електронний ресурс]
URL: https://sumy.univd.edu.ua/science-issue/issue/4225

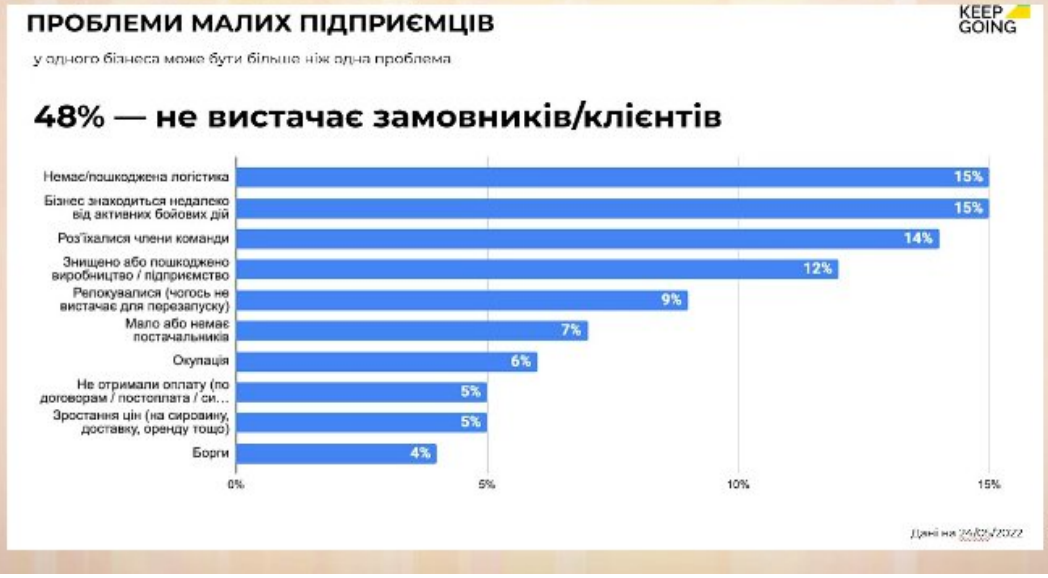
Додаток А.

КОПІЇ СЛАЙДІВ МУЛЬТИМЕДІЙНОЇ ПРЕЗЕНТАЦІЇ





Проблеми малого бізнесу



3

Внутрішні загрози. Вплив війни на малий бізнес

4

Зовнішні загрози

5

Загрози для малих компаній

Невеликі компанії найбільш схильні до кіберзагроз і можуть зіткнутися з наступними ризиками:

- розкрадання даних, зокрема персональних, а також технології, договори, бази клієнтів, інформація про поточні угоди;
- взлом або розкрадання сайту. Може бути дуже чутливо для компаній, які залучають основний потік клієнтів саме через інтернет;
- фішинг, завдяки якому можна отримати доступ до банківського рахунку або корпоративної банківської картки;
- віруси-здирники і шифрувальники, які не тільки вимагають грошей, а й гальмують усі робочі процеси.

6

Методи захисту

Антивірус	Швидше за все вже встановлено і головне, щоб він регулярно оновлювався.
Міжмережевий екран	Буває програмним, буває у вигляді окремого пристрою, який фільтрує трафік. Тут підійде Traffic Inspector Next Generation. У нього є версія для малого і середнього бізнесу.
Додаткова аутентифікація	Перш, ніж увійти в робочий комп'ютер співробітнику треба буде отримати СМС з перевірочним кодом. Особливо актуально для захисту робочих машин бухгалтера, директора або ключових співробітників. Просте рішення є у компанії ESET.
Моніторинг роботи співробітників	Може працювати і як DLP. Програма постійно стежить за пристроями співробітників: сайти, відкриті документи, продуктивність, копіювання файлів. Усе збирається в зручні звіти. Таким чином можна відстежити співробітників, які готові звільнятися. А за ними потрібен особливий контроль.
Комплексні рішення	Шифрування даних і резервне копіювання файлів Захист платежів Захист бізнес-додатків

7

Рекомендації щодо захисту малих компаній

- визначити цінність інформації та розподілити її за окремими мережевими папками і налаштувати до них доступ;
- налаштувати на кожному робочому пристрої доступ за логіном і складним паролем. В ідеалі паролі треба міняти раз на три місяці;
- провести повну інвентаризацію обладнання. Усе, що викликає підозри, має бути ізольовано і перевірено;
- провести повну інвентаризацію програмного забезпечення. Видалити все, що не стосується конкретних завдань співробітника;
- заборонити співробітникам встановлювати будь-яке програмне забезпечення;
- налаштувати систему подвійного резервного копіювання критично важливих даних: одна копія має зберігатися на фізичному носії в недоступному для співробітників місці, а друга - в захищеній хмарі;
- за можливості заблокуйте користувачам соцмережі та файлообмінні мережі, зокрема хмарні.

8

Яка інформація потребує захисту

Найчастіше на малих підприємствах доводиться захищати:

- відомості про клієнтів, постачальників, нові розробки та ноу-хау;
- зміст договорів із партнерами;
- собівартість продуктів і послуг;
- аналітичні та маркетингові дослідження, їхні результати та висновки;
- дані про фінансовий стан компанії та про зарплати.

9

Головні елементи організації інформаційної безпеки

№ п/п	Елемент схеми безпеки	Заходи
1	визначення вразливих місць	створення переліку всіх ресурсів, які мають бути захищені
2	визначення загроз	аналіз переліку можливих загроз для кожного окремого ресурсу
3	оцінка рівня загрози	побудова шкали рівнів небезпеки для кожного ресурсу, на основі можливих наслідків у випадку несанкціонованого доступу
4	контроль управління доступом	розподіл структурно-штатної схеми підприємства на категорії доступу до захищеної інформації
5	протидія	розробка заходів, скерованих на унеможливлення випадків несанкціонованого доступу до ресурсу з певним рівнем безпеки
6	впровадження	затвердження, впровадження та контроль за дотриманням заходів організації інформаційної безпеки підприємства
7	усунення наслідків	програма швидкого реагування на випадки несанкціонованого доступу до захищеної інформації, яка направлена на мінімізацію завдання шкоди підприємству

10

Спам-повідомлення та антиспам

Спам-повідомлення - це небажані листи, які надсилаються за допомогою електронної пошти. Отримання таких листів сповільнює роботу з електронною поштою та просто дратує. У зв'язку з цим спеціалісти рекомендують використовувати функцію Антиспам для фільтрування небажаних та шкідливих повідомлень.

Антиспам - це модуль програмного забезпечення, який запобігає та блокує небажані електронні листи, такі як спам.

Антиспам використовує різні засоби для фільтрування небажаних повідомлень, наприклад «білі» та «чорні» списки, списки адрес, авторитетні пошти та відповідні ключові слова. Спам-фільтр присвоює оцінку кожному просканованому повідомленню електронної пошти та використовує цей показник, щоб визначити доставляти повідомлення чи додати його до небажаної пошти.

11

ДЯКУЮ ЗА УВАГУ!

UNICHECK
by Turnitin

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015643038

Дата перевірки:
19.06.2023 11:33:01 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
19.06.2023 11:33:36 EEST

ID користувача:
100011688

Назва документа: 2БКС-27 Козак Микита

Кількість сторінок: 47 Кількість слів: 8476 Кількість символів: 65432 Розмір файлу: 3.25 MB ID файлу: 1015289223

18.6%
Схожість

Найбільша схожість: 11.8% з Інтернет-джерелом (http://dynamic-design.com.ua/novosti/uk/bezopasnost-osoblivosti-zab.

18.6% Джерела з Інтернету | 126 ..... Сторінка 49

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Козак Микита Олексійович,
здобувач освіти гр. 2БКС-27, та

Кільдішев Віталій Йосипович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Дослідження рівня безпеки малих підприємств з розробкою захисних мір» (автор роботи – Козак М.О., керівник роботи – Кільдішев В.Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Козак М.О. /

Керівник _____ / Кільдішев В.Й./

«16» червня 2023 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника про кваліфікаційну роботу бакалавра

Козака Микити Олексійовича

(прізвище, ім`я та по батькові здобувача/здобувачки освіти)

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи

«Дослідження рівня безпеки малих підприємств з розробкою захисних мір»

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) обсяг і якість виконання роботи (розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над кваліфікаційною роботою

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Провів аналіз можливості використання технічних засобів та методології раціонального вибору ТЗ забезпечення ІБ підприємства. В рамках застосування засобів захисту запропоновано використання технічних засобів охорони та спецзасобів щодо блокування каналів витоку відеоінформації.

в) теоретична підготовка бакалавра

відповідає вимогам, що надаються до бакалавра зі спеціальності «Комп'ютерна інженерія»

г) вміння розв'язувати виробничі та конструкторські питання _____

У кваліфікаційній роботі досліджується інформаційне середовище комерційного підприємства. Розглянуто роль підприємств малого та середнього бізнесу в структурі держави, наведено класифікації. Розглянуто загрози та ризики – як внутрішні, так і зовнішні.

Оцінка розрахункової частини добре

Оцінка графічної (презентаційної) частини добре

Загальна оцінка добре

Прізвище, ім'я, по батькові керівника роботи Кільдішев Віталій Йосипович

Місце роботи і посада керівника роботи к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

«15» грудня 2023 р. _____ _____

(підпис) (прізвище та ініціали керівника)

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Козака Микити Олексійовича

(прізвище, ім`я та по батькові)

Напрямку підготовки *123 «Комп'ютерна інженерія»*

Керівник кваліфікаційної роботи

Кільдішев Віталій Йосипович

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи

«Дослідження рівня безпеки малих підприємств з розробкою захисних мір»

Обсяг пояснювальної записки _____ сторінок

Обсяг графічної (презентаційної) частини проекту _____ аркушів (слайдів)

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаної роботи завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) характеристика виконання кожного розділу роботи

При виконанні дипломного проекту студент продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідив та проаналізував методів та засобів захисту комерційної таємниці сучасного підприємства.

в) оцінка якості виконання графічної (презентаційної) частини роботи і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Розглянута роль і значення захисту інформації у діяльності комерційного підприємства. Схематично показано взаємодію об'єктів захисту з видами зловмисників і службами підприємства. Розроблено основні способи усунення можливості шахрайства комерційного підприємства.

г) перелік позитивних якостей роботи _____

Тема дипломного проекту є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання. _____

_____

_____

д) основні недоліки роботи У тексті пояснювальної записки відсутні посилання на використану літературу, для підвищення ефективності захисту було б доцільним навести класифікацію внутрішніх і зовнішніх загроз в аспекті економічної безпеки підприємства. _____

_____

_____

Оцінка розрахункової частини Добре

Оцінка графічної (презентаційної) частини Добре

Загальна оцінка Добре

Прізвище, ім'я та по батькові рецензента Кривошеко Юрій Вікторович

_____

Місце роботи і посада рецензента ОТФК ОНТУ

асистент каф. комп'ютерної інженерії

_____

«16» червня 2023 р. _____ Кривошеко Ю.В.

(підпис) (прізвище та ініціали рецензента)