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.27.02.000.КРБ

Андріяненко Олексія Юрійовича

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:

«Аналіз методів та засобів щодо захисту комерційної таємниці сучасного підприємства»

Проектний матеріал складається з пояснювальної записки на 63 сторінках та графічного (презентаційного) матеріалу на 14 аркушах (слайдах)

Виконавець _____ (Андріяненко О.Ю.)
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 «24» 06 2023 р. Протокол ДКК № 2
Оцінка ДКК 4 (добре)

Секретар ДКК _____

АНОТАЦІЯ

Метою даної роботи є аналіз методів та засобів щодо захисту комерційної таємниці сучасного підприємства.

У бакалаврській роботі розглянуто роль підприємств малого та середнього бізнесу в структурі держави, наведено класифікації. 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 технічних засобів охорони та спецзасобів щодо блокування каналів витоку відеоінформації. В рамках захисту корпоративної мережі використовуються системи протидії витокам (DLP) та додаткові методи з позиції NIST 7621.

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 Андріяненко Олексію Юрійовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи
Аналіз методів та засобів щодо захисту комерційної таємниці сучасного підприємства

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

2. Термін здачі кваліфікаційної роботи 15 червня 2023 р.

3. Вихідні дані до роботи Міжнародна нормативно-правової бази щодо захисту комерційної таємниці. Аспекти захисту комерційної таємниці в Україні. Аксіоми резервного копіювання. Способи протидії автоматичному збору персональних даних з інформаційного ресурсу.

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

Вступ. 1. Формування класів ризику комерційної таємниці. 2. Алгоритми формування системи захисту комерційної таємниці. 3. Аудит інформаційної безпеки. 4. Дослідження механізмів захисту персональних даних в мережі Інтернет. 5. Охорона праці. Висновки. Перелік використаних джерел. Додаток

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

Лист 1 – Визначення та класифікація правопорушень

Лист 2 – Класифікація інсайдерів Модель шкідливих дій інсайдера

Лист 3 – Глобальна екосистема інсайдерської діяльності

Лист 4 – Організаційно-технічні заходи щодо забезпечення комерц. таємниці

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	*Черновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання Кільдішев В.Й.

Керівник роботи _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1	Вступ. Практичні аспекти щодо захисту комерційної таємниці	**24.05.2023 р.**	ВИКОНАВ
2	Стратегія захисту комерційної таємниці в інформаційних системах	**26.05.2023 р.**	ВИКОНАВ
3	Розробка концепції захисту комерційної таємниці	**01.06.2023 р.**	ВИКОНАВ
4	Методи захисту персональних даних в мережі Інтернет	**03.06.2023 р.**	ВИКОНАВ
5	Виконання розділу «Охорона праці»	**08.06.2023 р.**	ВИКОНАВ
6	Виконання графічної частини роботи	**13.06.2023 р.**	ВИКОНАВ
7	Чистове оформлення пояснювальної записки кваліфікаційної роботи	**15.06.2023 р.**	ВИКОНАВ
8	Підготовка доповіді та презентації для захисту	**17.06.2023 р.**	ВИКОНАВ
9	Отримання рецензії, відповіді на зауваження рецензента	**21.06.2023 р.**	ВИКОНАВ
10	Захист роботи	**23.06.2023 р.**	ВИКОНАВ

Виконавець _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27.02.000.00 КРБ	*Кваліфікаційна робота*		
А4			БКС 27.02.000.00 КРБ ПЗ	*Пояснювальна*	*1*	
				записка		
			БКС 27.02.000.00 КРБ МП	*Мультимедійна*		
				презентація		

Ізм.	Арк.	№ докум.	Підпис	Дата	*БКС 27.02.000.00 КРБ ПЗ*		
Розробив		Андріяненко О.Ю.			Аналіз методів та засобів щодо захисту комерційної таємниці сучасного підприємства	Літ.	Аркуш
Перевірив		Кільдішев В.Й.				*Н Д П*	*3*
						ОТФК ОНТУ гр.БКС-27	
Н. Контр.		Петрашова В.І.					
Затверд.		Іванова Л.В.					

ЗМІСТ

ВСТУП

Витік конфіденційної інформації вкрай небезпечна для компанії. Це тягне за собою фінансові втрати, втрату репутації і навіть призводить до банкрутства підприємства. Сьогодні найголовніша загроза для підприємства - інсайдери: недбалий або ображений на керівництво співробітник або ті, хто свідомо працює на компанію-конкурента або підтримує зв'язок з кримінальними структурами. На рахунку цих осіб більшість гучних справ по крадіжці даних, зафіксованих в світі останнім часом.

Звичайно, багато інформації «витікає» через недбалість працівників. Вже на стадії тестування систем інформаційної безпеки SearchInform з'ясувалося, що близько 70% співробітників (найчастіше ненавмисно) обмінюються з особами поза компанією корпоративними даними про зарплати, планованих рекламних акціях, стратегіях продажів і т.д. «Виявилася» і така тенденція: переходячи з однієї фірми в іншу (суміжну за видом діяльності), співробітники вже навмисне забирають із собою файли, часто становлять комерційну таємницю.

Боротьба з витоками інформації - вимушена необхідність в сучасних умовах ведення бізнесу. Головне при цьому - комплексний підхід. Утім, вважається, що багато підприємств якщо і використовують схему захисту інформації, то тільки «часткову», тобто застосовують різнорідне ПЗ, щоб за фактом закрити «дірки» в корпоративної комп'ютерної мережі («обрізають» доступ співробітників до соціальних мереж, всіляких месенжерів, блокують USB-пристрої та ін.). Але про комплексну захисту мова, як правило, не йде. Питання впровадження СЗІ для захисту від внутрішнього порушника досить актуальне, бо згідно статистичних показників на внутрішні порушення інформаційної безпеки наводиться близько 80% всіх порушень.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Дослідження екосистеми інсайдера як глобальної внутрішньої загрози

1.1.1 Щодо проблематики інсайдерства та внутрішніх загроз

Розвиток сучасного суспільства стає все більш залежним від стрімкого впровадження інформаційних технологій у всі сфери нашого життя. Інформація та людський фактор стають тими системами, захист яких є найважливішим в інформаційній безпеці підприємства. Інформація може бути підроблена, втрачена, викрадена, пошкоджена, знищена не лише зовнішніми порушниками. Зловмисні, недбалі та скомпрометовані користувачі компаній становлять не менший ризик, який на сьогодні має тенденцію зростати. Як показує Глобальний звіт про витрати на внутрішні загрози за 2022 рік:

- інциденти з інсайдерськими загрозами зросли на 44% за останні два роки;
- витрати на інцидент зросли більш ніж на третину до 15.38 мільйона доларів;
- вартість крадіжки облікових даних для організацій зросла на 65% з 2,79 мільйона доларів у 2020 році до 4.6 мільйона доларів на даний момент;
- час стримування інциденту з внутрішньою загрозою збільшився з 77 днів до 85 днів, що змусило організації витрачати найбільше на стримування;
- інциденти, які зайняли понад 90 днів, щоб стримати витрати організацій, у середньому становили 17.19 мільйонів доларів США на річній основі.

Інша аналітична статистика «Insider Threats: 20 Alarming Facts and Figures» [2] підкреслює, що 25% співробітників використовують електронну пошту, щоб

вилучити конфіденційні дані компанії: 34% глобальних компаній страждають від внутрішніх загроз: 50% організацій вважають, що вони вразливі до інсайдерських атак: 55 % організацій вважають привілейованих користувачів найбільшим ризиком внутрішньої загрози: 97% IT-лідерів вважають інсайдерські загрози серйозною проблемою безпеки.

Атаки з боку інсайдерів, будь-то співробітники, постачальники чи інші компанії, законно підключені до комп'ютерної системи компанії, становлять більш згубну загрозу, ніж зовнішні атаки. Ці інсайдери мають знання про внутрішню роботу організації та повністю володіють усіма правами та привілеями, необхідними для здійснення атаки, яких не вистачає стороннім особам. Отже, інсайдери можуть зробити свої атаки звичайними операціями.

1.1.2 Основні поняття та ознаки інсайдерської інформації

Поняття «інсайдерська інформація» в наукових колах розглядають з різних сторін правового поля, найчастіше на інтуїтивному рівні:

– істотна, публічно не розкрита інформація до певного часу;

– особливий різновид службової таємниці;

особливий вид інформації з обмеженим доступом.

Інсайдерською може бути, наприклад, інформація щодо злиття чи розпаду компаній; фінансові звіти підприємства: інформація, яка може вшишути на бізнес-процеси компанії: істотні зміни у планах капіталовкладень товариства: операції зі значними активами емітента за неринковою ціною: знищення або пошкодження значної частини майна емітента внаслідок непередбачуваних подій тошо [6].

В Директиві Ради Європейських Співтовариств від 13 листопада 1989 року 89/592/ЄЕС інсайдерська інформація визначається як інформація, яка не була розголошена, має чітку форму і відноситься до одного чи декількох емітентів

цінних паперів, що підлягають обігу або стосується одного чи декількох цінних паперів, що підлягають обігу, та розголошення якої вірогідно матиме суттєвий виліт на ціну відповідного цінного паперу чи паперів, що підлягають обігу [8].

В Україні вперше поняття «інсайдерської інформації» набуло юридичної сили у Законі "Про цінні папери та фондовий ринок" від 23.02.06 р. [5]: інсайдерська інформація - неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених цим Законом. Інформація щодо оцінки вартості цінних паперів та/або фінансово-господарського стану' емітента, якщо вона отримана виключно на основі оприлюдненої інформації або інформації з інших публічних джерел, не заборонених законодавством, не є інсайдерською інформацією. Інформація не вважається інсайдерською з моменту її оприлюднення відповідно до закону. Перелік відомостей, віднесених до інсайдерської інформації, визначається Державною комісією з цінних паперів та фондового ринку.

Інсайдерську інформацію слід відрізняти від комерційної таємниці. «Документи про неплатоспроможність підприємства (наприклад, за результатами проведеного аудиту), інформація про забруднення навколишнього природного середовища (за яке підприємство може бути покаране як штрафами, так і зобов'язанням відшкодувати заподіяні збитки) та інша інформація, яка не може бути комерційною таємницею, ймовірно може викликати падіння ринкової вартості цінних паперів відповідного емітента після її оприлюднення. А отже, до моменту оприлюднення вона може бути інсайдерською інформацією» [9].

Підсумовуючи вище викладене, можна вважати, що основними ознаками інсайдерської інформації є істотність (комерційна цінність), непублічність. релевантність.

1.1.3 Екосистема та характеристики інсайдера

Аналіз наукових джерел дозволив зробити висновок, що точного визначення поняття «інсайдер» не існує, кожен дослідник розробляє власне тлумачення, яке є специфічним дія його власного набору даних, ситуацій, упереджень і припущень. Зупинимося на деяких з них.

Банківська енциклопедія трактує поняття «інсайдер» (англ. insider- всередині) - особа, яка завдяки своєму службовому становищу або спорідненим зв'язкам має доступ до конфіденційної інформації про діяльність банку, що недоступна широкій громадськості та може використати її у власних цілях з метою збагачення, одержання неконкурентних переваг, привілеїв тощо [10]. Далі перераховуються належність фізичних і юридичних осіб до класу інсайдєрів.

Автори дослідження [11] пропонують розширити це поняття, враховуючи питання кібер- та фізичної безпеки. Інсайдер може бути визначений щодо двох примітивних дій:

- порушення політики безпеки з використанням легітимного доступу:

- порушення політики контролю доступу шляхом отримання несанкціонованого доступу.

У першому випадку інсайдер використовує свій законний доступ для виконання певних дій. які суперечать політиці безпеки, наприюіад. коли конфіденційні дані передаються третім особам або коли доступ до ресурсу надається чи блокується. У другому випадку інсайдер використовує свій доступ

дня розширення своїх привілеїв таким чином, що порушує політику контролю доступу та безпеки.

Близьке поняття зустрічаємо у науковій праці [12]: інсайдер - довірена особа, якій надано повноваження порушувати політику безпеки.

Як стверджує група науковців [13]: інсайдерами можуть бути колишні чи незадоволені працівники чи будь-який діловий партнер, який має чи мав санкціонований доступ до інформації для будь-якої конкретної організації. Вони мають заходи контролю та безпеки.

У роботі [14] дотримуються наступного визначення: інсайдери — це авторизовані користувачі, які мають законний доступ до конфіденційної інформації і вони можуть знати уразливі місця розгорнутих систем і бізнес-процесів.

Сучасні інформаційні потоки ініціюють створення так званих «структурних інсайдерів». Як стверджується в [15], «структурні інсайдери» - високошвидкісні трейдери, які купують і продають цінні папери за мілі- та мікросекунди. Цьому має сприяти декілька умов: близьке розташування з серверами біржі: постійні інформаційні потоки між біржами і трейдерами: автоматична відповідь на нові інформаційні масиви. Все це вимагає швидкодійних алгоритмів дтя обробки великих масивів даних у режимі реального часу. Таким чином, перевага «структурних інсайдерів» в тому, що вони першими отримують новітню інформацію та торгують нею. а сторонні особи змушені здійснювати операції із застарілими даними та старими цінами.

З метою створення «портрету інсайдера» узагальнимо його ключові характеристики:

- інсайдери мають легітимний доступ до конфіденційної інформації: знають уразливості інформаційних активів;

- мають добре сформовані навички для здобуття цінної інформації;

- інсайдери завжди мотивовані (матеріальна сторона або емоційне невдоволення та помста).

У науковій роботі [16] підкреслюється, що для здійснення інсайдерської атаки мають бути одночасно три елемента: мотив, здатність, можливість.

Визначення окреслених ознак «портрету інсайдера» дає можшівість сформувати поняття «інсайдерська діяльність». Інсайдерська діяльність - спрямовані дії мотивованігх суб'єктів, які мають легітимний доступ до інформаційнігх активів та навички для здобуття цінної інформації', знають уразливі місця шформаціїїних систем і бізнес-процесш. для завдання матеріальних збитків та/або реп)лаціїппгх втрат організації.

Варто відзначити, що в більшості випадків під словом "інсайдер" мають на увазі "внутрішнього зловмисника". Принаймні, таке вживання склалося спочатку, як тільки почалося активне обговорення та висвітлення теми інсайдерів у пресі.

Проте абсолютно незрозуміло, чому сьогодні змішують поняття "діючого внутрішнього зловмисника", "потенційного внутрішнього зловмисника", "недбалого співробітника" і "зовнішнього зловмисника", який проник всередину мережі, що захищається. Журналісти та експерти звертають дедалі менше уваги на те, що термін "інсайдер" став розмитим і змішався з абсолютно чужими поняттями. Сьогодні до інсайдерів відносять:

– співробітників, які втрачають ноутбуки, кишенькові комп'ютери і переносні HDD з конфіденційними даними;

– підкуплених прибиральниць, які, наводячи лад у кабінеті перших осіб компанії, зламують парольний захист комп'ютера, знаходять конфіденційну інформацію і копіюють її на USB-флешку;

– підкуплених або обмежених у своїх інтересах співробітників, які крадуть конфіденційні дані, нехтуючи всіма моральними нормами;

– співробітників, які навмисно або випадково запускають в корпоративну мережу шкідливу програму і т.д.

Побіжний погляд на наведені приклади та зіставлення фактів з чітким визначенням поняття "інсайдер" показують, м'яко кажучи, невідповідність його коректного значення і поширених вживань. Однак подібні помилки ─ норма в сучасних дискусіях з інформаційної безпеки.

Ось чому необхідно чітко визначити для себе поняття "інсайдер", перш ніж довірятися лякаючій статистиці інцидентів і тим більше, перш ніж купувати "засіб боротьби з інсайдерами".

Отже, інсайдер - це людина, допущена до роботи з інформацією, призначеної для строго обмеженого кола осіб. І тільки. Ніяких прибиральниць і флешок, ніяких крадіжок ноутбуків і ніяких розваг на роботі.

1.1.4 Класифікація інсайдерів

Існує декілька підходів до класифікації внутрішніх порушників. Один з перших кроків у цьому напрямку зробила компанія IDC, яка представила своє бачення проблеми два роки тому. За версією IDC, екосистема інсайдерів має чотири рівня: «громадяни», «порушники», «відступники», «зрадники».

Верхній рівень складають «громадяни» - лояльні службовці, які дуже рідко (якщо взагалі колись) порушують корпоративні політики та в основному не є загрозою безпеці. «Порушники» складають більшу частину «населення» корпорації. Ці співробітники дозволяють собі невеликі фамільярності, працюють з персональної веб-поштою, грають в комп'ютерні ігри і здійснюють онлайн-покупки. Представники даного шару становлять загрозу IT-безпеки, але супутні їм інциденти є випадковими і ненавмисними. На наступному щаблі знаходяться «відступники» - працівники, які проводять більшу частину дня, роблячи те, що

вони робити не повинні. Ці службовці зловживають своїми привілеями з доступу до інтернету, самовільно встановлюють і використовують P2P-клієнти і IM-додатки. Більше того, такі співробітники можуть відсилати конфіденційну інформацію компанії зовнішнім адресатам, зацікавленим в ній. Таким чином, «відступники» представляють серйозну загрозу IT-безпеки. Нарешті, на самому низу знаходяться «зрадники». Це службовці, навмисне і регулярно піддають конфіденційну інформацію компанії небезпеки. Зазвичай за фінансову винагороду від зацікавленої сторони. Такі співробітники представляють найнебезпечнішу загрозу. Одночасно, їх складніше всього зловити.

Серйозний недолік цієї класифікації - відсутність повної картини. Розділити співробітників на групи і вказати, чим вони займаються на робочому місці - всього лише пів справи. За рамками залишилися такі важливі моменти, як цілі, мотивації, послідовність дій, методи. А головне, немає чіткої прив'язки класифікації до проблеми захисту конфіденційності та цілісності інформації. Адже саме це найбільше хвилює компанії, а зовсім не те, якими іграми захоплюються співробітники.

Також інсайдерські правопорушення (злочини) можна класифікувати за такими характерним напрямами (з точки зору основних параметрів розслідування злочину):

по виду предмета інтересів для розкрадання / впливу:

– інформація,

– ношений (транспортабельний) предмет,

– складна технічна установка, інформаційний вплив на яку може призвести до значних втрат,

– інформаційна система з важливою інформацією,

– інформаційна система управління системою безпеки,

– співробітник;

за якісним складом інсайдерів:

– одиночний,

– група інсайдерів,

– одиночний у змові з зовнішнім,

– група інсайдерів у змові з зовнішнім;

по усвідомленості дій:

– навмисні (повністю усвідомлювані),

– недбалі, хуліганські (частково усвідомлювані),

– неусвідомлені;

за типом інсайдера:

– впроваджений агент,

– колишній злочинець,

– співробітник з психічними аномаліями,

– співробітник, який отримав психічні аномалії під час роботи,

– співробітник, поміняв своє правосвідомість під час роботи;

по мотивацію вчинення:

– отримання особистої вигоди,

– інтерес (крадіжка інформації з метою подивитися, зламати),

– байдужість,

– бажання помсти,

– дії під примусом,

– ідеологічний (політичний),

– самореалізація, підвищення адреналіну;

за посадовими можливостями:

– без можливості доступу до об'єкта інтересів (ОІ),

– з періодичною / постійною можливістю доступу до ОІ без нагляду / під наглядом,

– забезпечує керування доступом до ОІ,

– розробляє систему управління доступом до ОІ;

по виявленню після вчинення або за фактом підготовки:

– миттєво,

– за фактом випадкового сприйняття, доступу,

– за фактом чергового контролю,

– за фактом розслідування,

– ніколи;

за ступенем покарання / впливу при виявленні:

– підпадають під статтю Кримінального кодексу,

– підпадають під адміністративне покарання на об'єкті,

підпадають під громадський осуд.

Рисунок 1.1 - Класифікація інсайдерських правопорушень

Згідно прийнятому в професійному середовищі баченню (Infowatch), виділяється 6 типів інсайдерів. Екосистема також включає такі параметри, як намір, користь, постановка завдання та дії при можливості. Класифікація представлена в табл.1.1.

Дана класифікація не включає більш дрібні групи інсайдерів, а також тих внутрішніх порушників, які не користуються корпоративною інформаційною системою. Ще одна з класифікація представлена на рис.1.2, де в легкій асоциативній формі представлено назви, які можна добре запам'ятати типи і розрізняти їх.

Таблиця 1.1 – Базова класифікація інсайдерів

Тип	Намір	Користь	Постановка завдання	Дії при неможливості
Недбалий	ні	ні	ні	повідомлення
Маніпульований	ні	ні	ні	повідомлення
Скривджений	так	ні	сам	відмова
Нелояльний	так	ні	сам	імітація
Сумісник	так	так	сам/ззовні	відмова /імітація/злам
Впроваджений	так	так	ззовні	злам

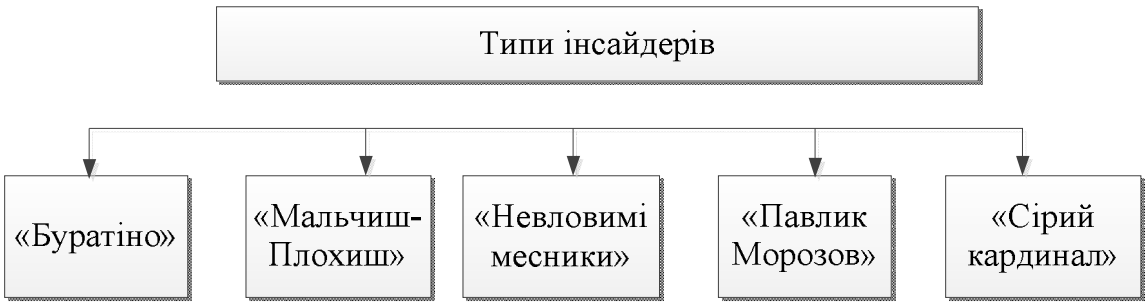


Рисунок 1.2 - Типи інсайдерів

1. *"*Буратіно*"* – відрізняє цікавість і прагнення сунути ніс не в свою справу. Цей тип інсайдера характеризується тим, що навіть якщо за родом своєї діяльності він не повинен мати доступу до конфіденційних даних, він все одно бажає з ними ознайомитися.

2. “Мальчиш-Плохиш*”* – легальний співробітник, який має право доступу до основного сервера, але недостатні повноваження для доступа до конфіденційної інформації. Така людина може спробувати підвищити недостатній для своїх цілей, не пов’язаних із роботою, рівень повноважень у серверної оперативної системи, до рівня адміністратора.

3. *“*Невловимі месники*”* – ображений або звільнення співробітників, який може скористатися періодом часу до відкликання адміністратором його прав доступу до конфіденційних даних, для їх копіювання або зміни з метою хоч якось “відігратися” за свої образи.

4. *“*Павлик Морозов*”* – легальний співробітник компанії, що діє цілеспрямовано і здатний залучати значні технічні ресурси для отримання доступу до інформації, що його цікавить. При цьому він використовує і соціальну інженерію, і фізичний доступ до сервера, і інші можливості, 90% із яких повністю легальні і необхідні для його штатної діяльності.

5. “Сірий кардинал” – зазвичай системний адміністратор, який за посадою має найвищий рівень прав доступу. Це найскладніший тип інсайдера з точки зору боротьби з ним.

Небезпека інсайдерської загрози, в цілому, полягає в тому, що співробітник підприємства на відміну від зовнішнього порушника володіє наступними характеристиками:

– знання та посадові повноваження,

– зв'язку і можливість отримання інформації від інших співробітників,

– можливість очікування найбільш «зручного» (відомого і очікуваного) моменту вчинення: профілактичні роботи, тимчасове делегування більших повноважень та ін.,

– велика можливість вступу в змову з іншими співробітниками з «відсутніми» для акції посадовими повноваженнями.

При цьому завжди є багато груп співробітників, які можуть вчинити будь-який злочин виходячи із сукупності їх посадових повноважень.

Проте варто зазначити, що вчинення злочину може відбутися тільки при наявності трьох умов:

– нагальна потреба,

– психологічна готовність,

– можливість бездоказового вчинення.

При цьому відсутність хоча б одного з цих умов призводить до неможливості здійснення злочину. На рис. 1.3 представлена модель шкідливих дій інсайдера.

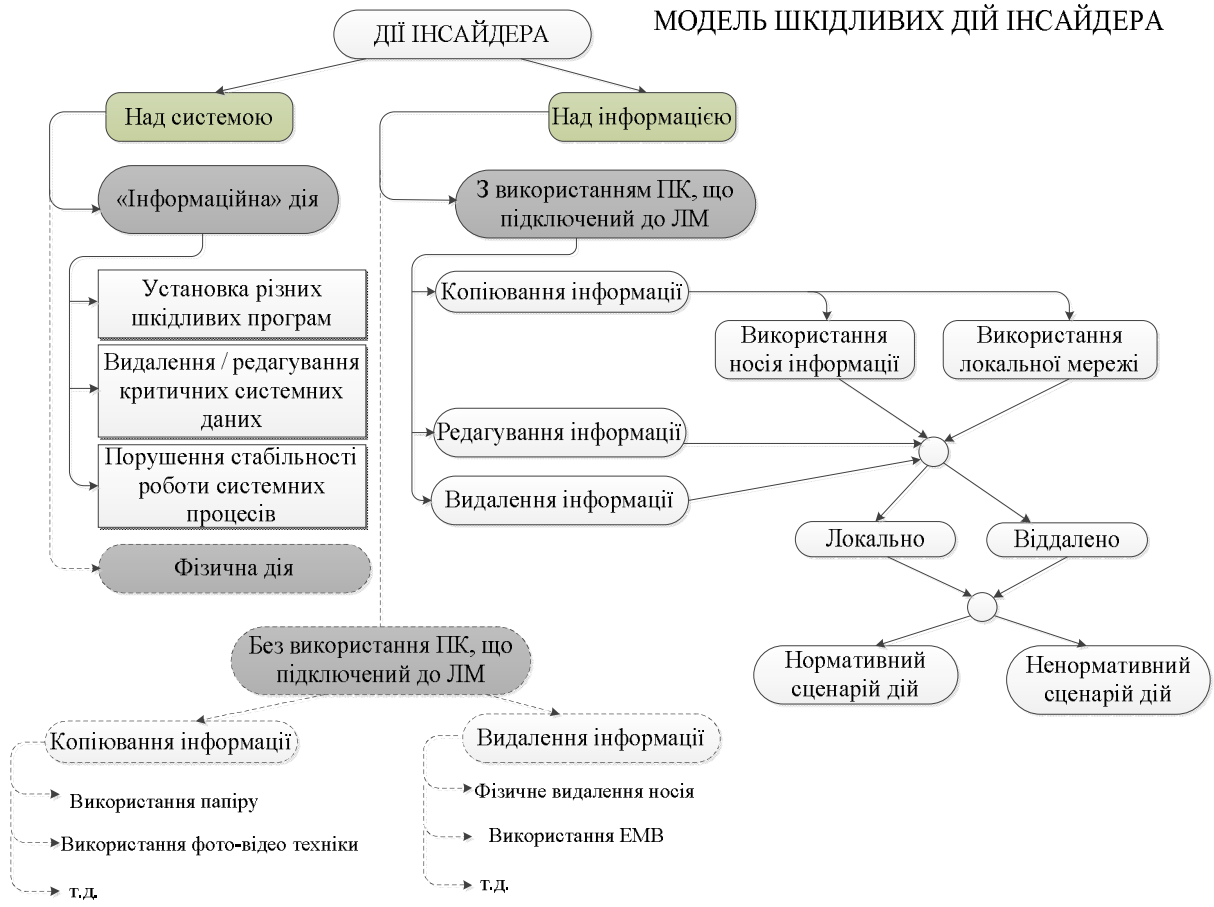


Рисунок 1.3 – Модель шкідливих дій інсайдера

1.1.4 Алгоритми виявлення інсайдерських загроз

Інсайдерська загроза проявляється, коли поведінка людей відходить від усталеної політики, незалежно від того, чи є вони результатом злоби, ігнорування чи незнання [17]. Інсайдерська загроза - це сукупність факторів, які можуть становити причину небажаного інсайдерського інциденту.

Вчені неодноразово підкреслювали вагомість емпіричних даних для моделювання та розроблення алгоритмів виявлення внутрішніх загроз. Джерелами для таких даних можуть слугувати [4]:

- реальні дані системного журналу;
- дані соціальних мереж;
- змодельовані дані, отримані зі стохастичних моделей;
- реальні дані з синтетичними аномаліями;
- змодельовані дані, отримані зі стохастичнігх моделей, розроблених на основі реальних даних;
- теоретико-ігровий підхід.

Удосконалення апаратнігх та програмних засобів захисту інформації дозволяють виділити джерела даних внаслідок моніторингу на основі хоста та мережі які мають відношення до виявлення внутрішньої загрози: записи реєстру, дозволи на файли, події системи виявлення вторгнень (IDS), доступ до облікового запису, журнали брандмауера, перехоплення вмісту електронної пошти, журнали сервера доменних імен (DNS)/доступ до Інтернет-сайтів, обмін миттєвими повідомленнями, відома сигнатура програмного забезпечення [17].

Разом з тим. перевіряючи здатність виявляти інтрузивну поведінку у внутрішньому середовищі, необхідно подбати про придушення частоти помилкових тривог. Вирішення даного питання пропонується у роботі [4] із застосуванням ймовірнісного підходу, який ілюструє частоту виникнення події у

відсотках, при цьому враховуючи частоту помилкових тривог на прийнятному рівні.

Узагальнення наукового доробку засвідчило, що у науковій літературі сформувалось декілька підходів до діагностики виявлення та прогнозування внутрішніх загроз. Так, у дослідженні [4] здійснено огляд алгоритмів виявлення та прогнозування внутрішніх загроз. Ці алгоритми поділяються на 6 категорій моделей, які представлені у табл.1.2.

Так, робота вчених [17] продемонструвала підхід прогнозного моделювання до пом'якшення внутрішньої загрози, який має на меті об'єднати різноманітний набір джерел даних не лише кібер-сферу, а також психологічні/мотиваційні фактори, які можуть лежати в основі зловмисних інсайдерських дій. Система CHAMPION (Columnar Hierarchical Autoassociative Memory Processing In Ontological Networks) містить ієрархічну структуру міркувань, організовану семантичним шаром, який забезпечує теоретико-графові методи розпізнавання образів. Ця комплексна система оцінки загроз автоматизує виявлення високоризикованих видів поведінки («попередників» або «тріперів»), на яких можна зосередити увагу та надати цей аналіз персоналу з кібербезпеки, які в іншому випадку повинні були б аналізувати та співвідносити величезну кількість даних.

Таблиця 1.2 – Алгоритми виявлення та прогнозування внутрішніх загроз

Назва моделі	Опис
Модель намірів (IM)	Впровадження психосоціальннх покажчиків на основі психологічних профілів інсайдерів
Модель поведінки особистості (IBM)	Внаслідок минулої інформації шодо діяльності інсайдера створюється його модель поведінки
Модель поведінки спільноти (CBM)	Внаслідок минулої інформації шодо цілої групи інсайдерів створюється модель поведінки
Модель використання ресурсів (RUM)	Внаслідок аналітичних даних щодо використання інсайдерамн якогось інформаційного ресурсу будується відповідна модель
Модель можливостей (CM)	Внаслідок статистичних даних шодо використання інсайдером різних рівнів IT-ресурсів моделюється відповідна діяльність
Змішана система (MS)	Технологія включає декілька моделей

Проте, як свідчить огляд представленої літератури, ще не розроблено жодних системних методів, комплексних технологій, які б забезпечували повніш та ефективніш підхід до запобігання витоку даних, саботажу, шпигунства та диверсій.

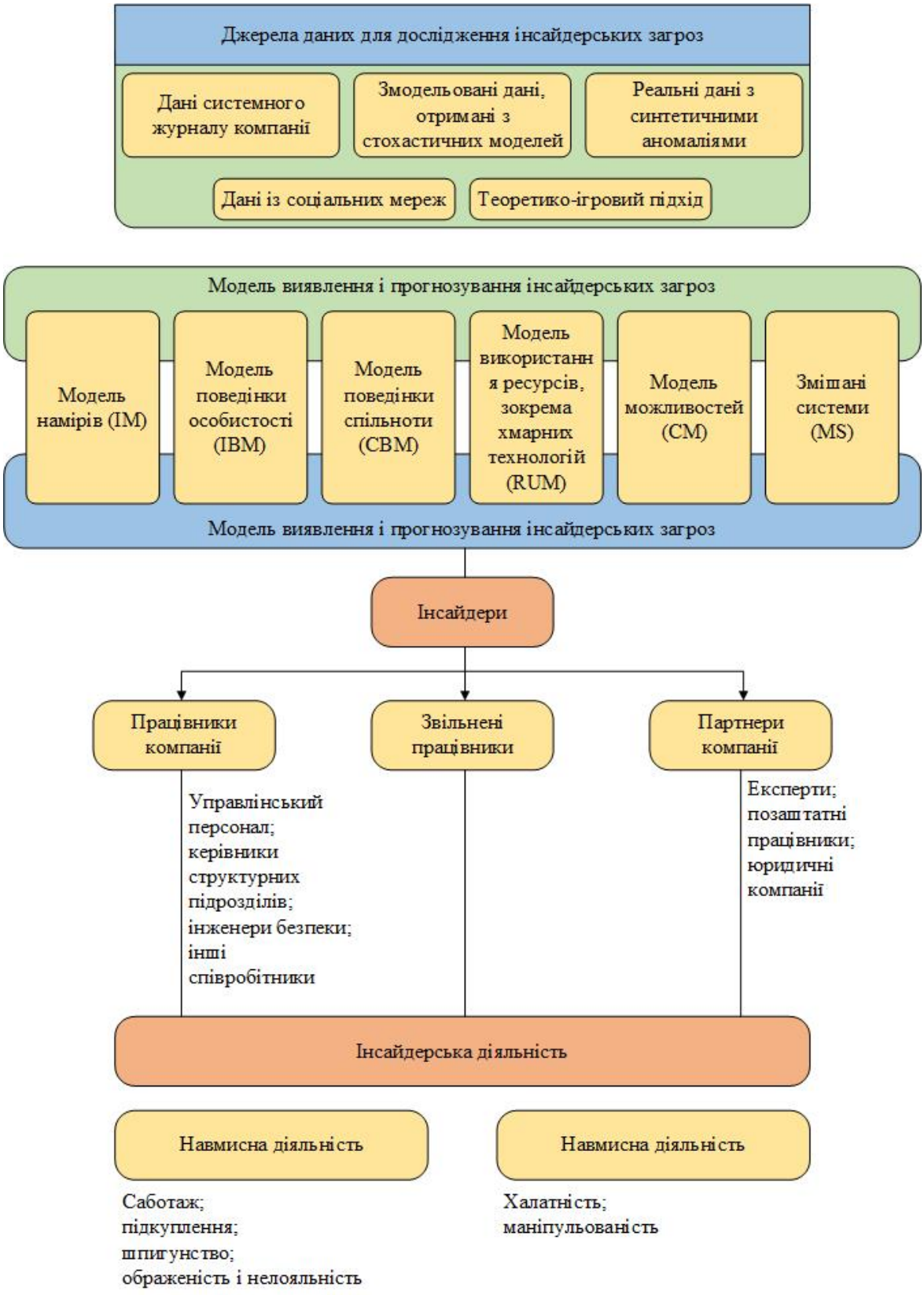


Рисунок 1.4 - Глобальна екосистеми інсайдерської діяльності

1.2 Організаційно-технічні заходи щодо забезпечення збереження комерційної таємниці на підприємстві

1.2.1 Пропозиції щодо формування механізмів захисту комерційної таємниці підприємства

Базові засоби захисту комерційної таємниці можна класифікувати на зовнішні та внутрішні, які, в свою чергу, поділяються на правові, організаційні, технічні та психологічні (рис. 1.5).

Рисунок 1.5 – Базові засоби захисту комерційної таємниці

Як і всі співробітники фірми, менеджер повинен при вступі і на роботу підписати зобов’язання про нерозголошення комерційної таємниці (про відповідальність за її збереження). Обов’язки роботодавця і працівника в цілях охорони конфіденційності інформації, що становить комерційну таємницю представимо у табл.1.3.

Таблиця 1.3 – Обов’язки роботодавця і працівника в цілях охорони конфіденційності інформації, що становить комерційну таємницю

Обов'язки	
Роботодавця	Працівника
Ознайомити під розписку працівника з переліком інформації, що становить комерційну таємницю	Виконувати встановлений роботодавцем режим комерційної таємниці
Ознайомити під розписку працівника з встановленим роботодавцем режимом комерційної таємниці і з заходами відповідальності за її порушення	Не розголошувати конфіденційну інформацію, власниками якої є роботодавець і нею контрагенти, і без їх згоди не використовувати цю інформацію в особистих цілях а протягом усією терміну дії режиму комерційної таємниці, в тому числі після припинення дії трудового договору
Створити працівникові необхідні умови для дотриманням ним встановленого роботодавцем режиму комерційної таємниці	Відшкодувати завдані роботодавцю збитки, якщо працівник винен у розголошенні інформації, що становить комерційну таємницю і стала йому відомою у зв'язку з виконанням ним трудових обов'язків
	Передати роботодавцю при припиненні або розірванні трудового договору матеріальні носії інформації, наявні в користуванні працівника і містять інформацію, що становить комерційну таємницю

1.2.2 Використання методики оцінки кадрових ризиків

Оцінимо загрози та вразливості персоналу. До навмисним причин, на його думку, відносяться: некваліфіковане виконання операцій; недбалість, безвідповідальність, недисциплінованість, несумлінне ставлення до виконуваної роботи; недбалість, необережність, неакуратність. Обставинами появи цих причин є: схильність до розваг, пияцтву, наркотикам; заздрість, образа; марнославство, зарозумілість, завищена самооцінка, хвастощі; низький рівень професійної підготовки; зайва балакучість, звичка ділитися досвідом, давати поради. Створена методика призначена для використання при прийомі співробітника на роботу,

оцінка кандидата поєднується з співбесідою. У ході співбесіди співробітник відділу кадрів заповнює відповіді кандидата на питання

Результатом є процентний показник вразливості: від 0% (кандидат вразливий з точки зору безпеки, і являє загрозу інформаційній безпеці підприємства) до 100% (кандидат невразливий і не представляє загрози). На розсуд керівництва і служби інформаційної безпеки можуть бути виставлені мінімальні прохідні пороги для різних категорій співробітників. Категорювання співробітників необхідно для визначення сценарію оцінки кандидата і заповнення таблиці відповідей. Критерії можуть бути різними. Категорії співробітників можуть виглядати наступним чином:

1) Співробітники постійно працюють з КІ високого ступеня важливості;
2) Співробітники періодично працюють з КІ високого ступеня важливості;
3) Співробітники постійно працюють з КІ середнього ступеня важливості;
4) Співробітники періодично працюють з КІ середнього ступеня важливості;
5) Співробітники рідко працюють з КІ середнього ступеня важливості;
6) Співробітники періодично працюють з КІ низького ступеня важливості;
7) Співробітники рідко працюють з КІ низького ступеня важливості.

Категорії можуть бути об'єднані. Наприклад:

– I категорія включає в себе 1,2,3 позиції;
– II категорія - 4,5 позиції;
– III категорія - 6 і 7 позиції.

Оцінювати уразливість кандидата необхідно за факторами, які представлені у вигляді блоків. Так, балакучість можна оцінити в ході співбесіди або попросити розповісти історію на певну тему, наприклад, про те, як пройшов вчорашній день. Прагнення співробітника помститися керівництву або колезі може призвести до витоку інформації під час роботи або після звільнення невдоволеного працівника.

Оцінити ризик умислу можна, запитавши думку про минуле місце роботи (керівництво, взаємини в колективі). Деякі захоплення характерні частою взаємодією з людьми, що збільшує ризик витоку інформації. Такими хобі можуть бути походи в нічні клуби, групові спортивні, танцювальні клуби, туризм. Спокійні домашні хобі більш безпечні з точки зору інформаційної безпеки. Наявність шкідливих звичок підвищує ризик витоку інформації в неформальній обстановці, наприклад, в курилці під час перерв, в компанії, перебуваючи в стані алкогольного сп'яніння. Уважність так само може послужити показником в процесі оцінки персоналу. Розсіяний співробітник може втратити носії з конфіденційною інформацією, а значить, потенційно становить загрозу компанії. Уважність можна оцінити за допомогою спеціальних тестів.

Стресостійкість співробітника складніше вибити з колії, а значить, зловмисникові складніше домогтися інформації обмеженого доступу. Слабостійких до стресів співробітник погано контролює себе в нестабільному стані, що може призвести до розголошення конфіденційної інформації. Стійкість в стресових ситуаціях можна виявити методом стрес-інтерв'ю. Можна запропонувати нестандартну ситуацію і дізнатися про дії співробітника в ній.

Найважливішим показником особистісних якостей суб'єкта є наявність у нього загальних уявлень про необхідність захисту конфіденційної інформації. Особиста сторінка в мережі може багато розповісти про життя людини, його інтересах і моральних принципах. Тому аналіз сторінки доповнює оцінювання вищевказаних блоків особистісних якостей. Запити за прізвищем, ім'ям та по батькові в пошукових системах можуть дати будь-яку інформацію про людину. Виявлену інформацію необхідно інтерпретувати індивідуально в кожному випадку. Оцінювання відбувається за 4-бальною шкалою по кожному з показників:

0 - кандидат представляє надзвичайно високу загрозу інформаційній безпеці (надмірно балакучий, злопам'ятний, запальний, у вільний час часто знаходиться в оточенні великих компаній, неуважний, легко піддається маніпуляціям, без роздумів повідомляє таємниці);

1 - кандидат представляє велику загрозу інформаційній безпеці (відповідає розгорнуто, іноді допускає зайву інформацію, схильний до злопам’ятності, запальності, у вільний час більше схильний перебувати в оточенні великих компаній, більше схильний до неуважності, насилу піддається маніпуляціям, без роздумів повідомляє деякі деталі таємницею інформації);

2 - кандидат представляє невелику загрозу інформаційній безпеці (мова лаконічна, рідко допускає зайву інформацію, схильний до злопам’ятності, запальності, у вільний час більше схильний перебувати в колі сім'ї, іноді знаходиться в оточенні великої кількості людей, швидше уважний, із великими труднощами піддається маніпуляціям);

3 - кандидат не представляє загрози інформаційній безпеці (контролює свою промову, відповідає стисло, абсолютно не злопам'ятний, емоційно стійкий, у вільний час проводить у сімейному колі, уважний, стійкий до маніпуляцій, не повідомляє таємниці).

Після співбесіди відбувається розрахунок коефіцієнта уразливості кандидата - Р, виражений у відсотках, за формулою:

$$P = \frac{\sum_{I=1}^{N} p_i}{4N} \qquad (1.1)$$

де N - кількість виставлених оцінок (у тому числі оцінки «0 балів»);

p_i - кількість балів за і-у відповідь;

i - порядковий номер відповіді.

Припустимо, кандидат відноситься до другої категорії, за якої, як правило, оцінюються 2 критерію по кожному блоку. Оцінені 10 блоків, в кожному блоці по 2 оцінки. Значить N = 20.

Бали виставлені таким чином:

Питання	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Бал	2	1	2	3	1	2	0	1	0	3	3	2	1	0	1	0	3	2	1	1

Порахуємо суму балів (чисельник дробу)

$$\sum_{I=1}^{N} p_i = 2+1+2+3+1+2+0+1+0+3+3+2+1+0+1+0+3+2+1+1 = 29$$

Розрахуємо коефіцієнт уразливості кандидата - Р за формулою 1.

$$P = \frac{29}{4 \times 20} \times 100\% = 0{,}3625 \times 100\% = 36{,}25\%$$

Інтерпретація результату може бути такою: «Коефіцієнт дорівнює 36,25%. Показник нижче 50%, означає, що кандидат представляє загрозу інформаційній безпеці організації ». Таким чином, унікальність розробленої методики полягає, по-перше, в числовому результаті оцінки співробітника, яка складається за різними критеріями для оцінювання; по-друге, у можливості проводити оцінку в залежності від градації кандидата, що впливає на глибину перевірки; по-третє, в економічності, тому методика не вимагає великих фінансових, матеріальних і трудових витрат.

Таблиця 1.4 – Анкета для оцінки кандидата

Категорія співробітника			Досліджуваний блок	Питання. Інший показник оцінки
I	II	III		
✓	✓	✓	Зайва балакучість	Прохання розповісти про вчорашній день
✓	✓			«Ви товариська людина?»
✓				У ході співбесіди
✓	✓	✓	Прагнення помститися керівництву або колезі по роботі	«Ви легко вибачаєте людей?»
✓	✓			Думка про попереднє місце роботи
✓	✓	✓	Схильність до розваг, пияцтву, наркотикам	«Чим ви захоплюєтеся?»
✓	✓			«Як Ви ставитеся до проведення вільного часу у великій галасливій компанії?»
✓	✓	✓	Наявність шкідливих звичок	«Чи є у Вас шкідливі звички?»
✓	✓	✓	Уважність	Психологічне тестування «Коректурна проба» (Тест Бурдона)
✓	✓	✓	Схильність маніпуляціям (вплив з боку зловмисника)	«Наскільки складно змінити Ваше думку?»
✓	✓			Тест «Піддаються ми маніпуляції?» З книги Кіри Буреніної
✓				(Спроба маніпулювати)
✓	✓	✓	Некваліфіковане виконання операцій	Провокація на розголошення КІ (Сценарій для кожної посади продумується індивідуально)
✓	✓	✓		«Чи є у вашій роботі інформація, поширення якої обмежено?»
✓	✓	✓	Сторінка в соціальній мережі	Аналіз змісту анкети, повідомлень, фото- і відеоматеріалу
✓	✓			Список цікавих груп, сторінок, на які підписаний користувач
✓				Рівень конфіденційності сторінки
✓	✓		Звернення на попереднє місце роботи	Бесіда з керівником, співробітниками, які мають можливість дати характеристику співробітникам (секретар, вахтер)
✓			Запит за особистими даними в пошукових системах	Виявлена інформація інтерпретується індивідуально в кожному випадку

Таблиця 1.5 – Бали за відповіді кандидата

Кількість балів за відповідь				Сума балів
3	2	1	0	
Контролює свою промову, відповідає стисло	Мова лаконічна, рідко допускає зайву інформацію	Відповідає розгорнуто, іноді допускає зайву інформацію	Надмірно багато інформації	
Ні	Скоріше ні	Скоріше так	Так	
Позитивне	«Ображений» співробітник. Не схильний до помсти	Неможливо оцінити. відмовляється відповідати	«Ображений» співробітник. Схильний до помсти	
Передбачає постійна взаємодія з людьми	Передбачає періодичне взаємодію з людьми	Передбачає чітку взаємодію з людьми	Чи не припускає взаємодії з людьми	
Негативно	Скоріше негативно	Скоріше позитивно	Позитивно	
Відсутні	Тільки куріння	Тільки вживання алкоголю	Куріння і алкоголь	
76-100% - відмінне увагу	51-75% - гарне увагу	26-50% - середнє увагу	0-25% - погане увагу	
Не стресостійкий	Скоріше не стресостійкий	Скоріше стресостійкий	Стресостійкий	
Складно	Скоріше складно	Скоріше легко	Легко	
Не схильний (24-32 бали)	Скоріше не схильний (16-24 бали)	Скоріше схильний (9-16 бали)	Схильний (0-8 бали)	
Не схильний	Скоріше не схильний	Скоріше схильний	Схильний	
Присутній	Скоріше присутній	Не знає	Відсутні	
Зміст анкети позитивно характеризує її власника	Зміст анкети швидше позитивно характеризує її власника	Зміст анкети скоріше негативно характеризує її власника	Зміст анкети негативно характеризує її власника	
Список груп недоступний	Груп і сторінок мало (до 10), зміст яких позитивно характеризує її	Груп і сторінок небагато (10 - 20), зміст деяких негативно	Груп і сторінок багато (більше 20), зміст яких негативно характеризує її	

	власника	характеризує її власника	власника	
Сторінка під псевдонімом з мінімальною кількістю інформації	На сторінці вказана інформація, яка не дає повного уявлення про її кандидата	Сторінка доступна всім користувачам. Анкета достатньо заповнена	Сторінка доступна всім користувачам. Анкета достатньо заповнена	
Відгуки про кандидата позитивні	Відгуки про кандидата швидше позитивні	Відгуки про кандидата скоріше негативні	Відгуки про кандидата негативні	
Кандидат невразливий	Кандидат швидше невразливий	Кандидат швидше вразливий	Кандидат вразливий	

Результатом є числовий показник в інтервалі від 0 до 100%: результат 0% означає, що «кандидат уразливий, представляє загрозу інформаційній безпеці підприємства», 100% - «кандидат невразливий, не представляє загрози інформаційної безпеки».

1.2.3 Аналіз системи заходів по захисту КТ

Система заходів, що забезпечують охорону комерційної таємниці, містить у собі:

– облік і охорону деяких видів матеріалів і готових виробів (особливо дослідних зразків);

– правильну постановку діловодства (циркуляції, обліку, зберігання, знищення документів);

– контроль над засобами копіювання та розмноження документів;

– захист інформації в засобах зв'язку та обчислювальній техніці;

– охорону території підприємства або його основних будинків і споруджень;

– нагляд за відвідуванням підприємства сторонніми особами.

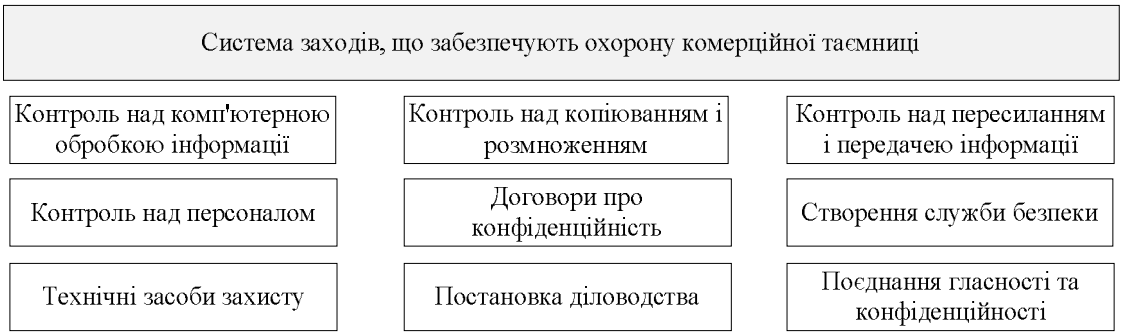


Рисунок 1.6 – Система заходів щодо захисту КТ підприємства

Одночасно з розвитком промислового шпигунства постійно вдосконалюються різноманітні засоби захисту комерційної таємниці. Так, у промислово розвинених країнах в останні роки постійно нарощує обсяги виробництва індустрія спеціальних технічних засобів захисту входу в службові приміщення. При цьому використовуються такі прогресивні нововведення, як картки з кодом, біометричні системи, що реагують на голос, підпис, відбитки пальців, візерунок кровоносних судин сітківки ока та т.п.

1.2.4 Алгоритм формування ”Положення про комерційну таємницю”

Як показує практика, більшість підприємців, а часом і їх начальників служб безпеки, дійсно вважають цей важливий документ простий даниною моді. «Положення» старанно викачуються з Інтернету, переписуються у друзів і ділових партнерів, а потім роками припадають пилом на полиці. Разом з тим, при правильному написанні і використанні даний документ є дієвим засобом захисту вашого бізнесу.

1.2.4.1 Розробка переліку відомостей, що становлять комерційну таємницю

Для ефективного захисту своїх секретів на першому етапі підприємець визначає перелік відомостей, що становлять комерційну таємницю підприємства. Як правило, для цього залучаються керівники структурних підрозділів, начальник служби безпеки і юрисконсульт (врахуйте, що в Постанові Кабінету Міністрів України від 09.08.1993 за № 611 законодавцем чітко визначені відомості, які не можуть становити комерційну таємницю).

В подальшому, для того, щоб узаконити цей перелік і використовувати його для захисту інтересів підприємства від зовнішніх і внутрішніх загроз, він офіційно віддається відповідним наказом директора. Другими наказом директора визначається перелік співробітників підприємства, допущених до відомостей, що становлять комерційну таємницю. Далі начальник служби безпеки (а при його відсутності - директора або його заступник) проводить ознайомлення зазначених співробітників до вимог двох наказів (під розпис). Перший етап роботи виконано. Ви офіційно задекларували наявність в своїй фірмі комерційних секретів і визначили осіб, допущених до них і є їх носіями.

1.2.4.2 Підготовка тексту ”Положення про комерційну таємницю”

Другим етапом є підготовка тексту «Положення про комерційну таємницю», зобов'язання співробітника про нерозголошення даних відомостей і наказу директора, що вводить їх на підприємстві. Тут начальник служби безпеки має можливість проявити всі свої знання, досвід і творчість.

В регламентній частини наказу вказати наступні вимоги:

− ввести в дію «Положення про комерційну таємницю»;

− співробітникам підприємства, допущеним до відомостей, що становлять комерційну таємницю, вивчити дане «Положення», підписати зобов'язання про нерозголошення комерційної таємниці і неухильно виконувати їх вимоги;

− передавати відомості, що містять комерційну таємницю підприємства (в усній формі, письмово, у вигляді документальних матеріалів, їх копій або в електронному вигляді) тільки з санкції директора, а при проведенні перевірок представниками контролюючих і правоохоронних органів - додатково після реєстрації перевіряючих в «Журналі реєстрації перевірок »;

− відповідальність за практичне здійснення режиму конфіденційності покласти на начальника служби безпеки (заступника директора), керівників відповідних структурних підрозділів і безпосередньо кожного із співробітників

В текст «Положення» доцільно включити такі розділи:

− загальні положення,

− правова база

− класифікація інформації

− режим конфіденційності

− відповідальність;

У тексті зобов'язання повинні бути вказані прізвище, ім'я, по батькові співробітника-секретоносія і його посада (як правило, заповнюються власноручно особою, як інструктується), місце для зазначення дати проведення інструктажу і підписи, як інструктували, так і особи, яка проводила інструктаж.

У змісті зобов'язання доцільно передбачити наступне:

− Співробітник усвідомив, що за родом виконання своїх посадових обов'язків він допущений до відомостей, що становлять комерційну таємницю підприємства;

− Співробітник зобов'язується, що як в період роботи на підприємстві, так

і протягом двох років після звільнення, він не буде розголошувати відомі йому «секрети» фірми;

− Співробітник згоден з тим, що всі результати його інтелектуальної роботи є власністю підприємства;

− В разі спроб сторонніх осіб отримати від співробітника відомості, що є комерційною таємницею підприємства, він зобов'язується негайно повідомити про це директору;

− Співробітник заявляє, що не має ніяких зобов'язань або угод з третіми юридичними або фізичними особами, які б суперечили даним зобов'язанням або обмежували його трудову діяльність в компанії;

− Співробітник ознайомлений з вимогами «Положення про комерційну таємницю» і зобов'язується неухильно виконувати викладені в ньому вимоги;

− Співробітник попереджений про те, що, в разі порушення вимог зобов'язання, він буде притягнутий до відповідальності у відповідності до чинного законодавства тощо.

1.2.4.3 Інструктаж персоналу

Третій етап - інструктаж персоналу. Як правило, його проведення покладається на начальника служби безпеки (а при його відсутності – на директора або його заступника). Не виконуйте ганебної практики, даючи співробітникам без інструктажу читати «Положення». У ньому викладено багато термінів і статей законодавства, які потребують додаткового роз'яснення. Разом з тим, на вимогу інструктували, йому повинна бути надана можливість самостійно ознайомитися з документом.

Необхідно пам'ятати, що головною метою інструктажу є усвідомлене розуміння таємниценосіями важливості забезпечення збереження комерційної

таємниці і формування почуття відповідальності за її розголошення, витік, втрату (починаючи від адміністративного покарання, в тому числі звільнення, аж до кримінальної відповідальності відповідно до ст. 231, 232 , 232-1, 361, 361-2, 362, 363 Кримінального Кодексу України). У зв'язку з цим після проведення інструктажу буде правильним поцікавитися, чи не виникли у співробітників питання, чи всі їм зрозуміло, а при необхідності - дати додаткові роз'яснення.

Інструктаж завершується індивідуальним ознайомленням співробітника з текстом зобов'язання і підписанням угоди інструктували та особою, яка проводила інструктаж, із зазначенням дати. Точно також не буде зайвим, якщо ваш співробітник поставить дату і свій автограф під текстом «Положення», тим самим підтвердивши факт проведення інструктажу.

За допомогою підготовленого таким чином пакету документів керівник підприємства має можливість дати мотивовану відмову на неправомірні вимоги представників контролюючих та правоохоронних органів про надання усної або письмової інформації, мінімізувати загрози для фірми при проведенні всіх видів перевірок, на законних підставах залучити до адміністративної або кримінальної відповідальності свого співробітника , що порушує вимоги конфіденційності або встав на шлях зради, а також ініціювати порушення кримінальної справи стосовно осіб, які займаються промисловим шпигунством. Правильно підготовлене і введене на підприємстві «Положення про комерційну таємницю» дозволить вашому персоналу не допускати помилок в різних кризових ситуаціях, в тому числі при незаконних домаганнях контролюючих та правоохоронних органів.

Не завадить передбачити заходи відповідальності прийнятих на роботу співробітників за розголошення комерційних секретів в укладених з ними трудових договорах / угодах. Як показує практика, питання забезпечення збереження комерційної таємниці необхідно відображати в договорах з різного роду клієнтами і діловими партнерами (в розділі «Обов'язки сторін»). Від фахівців

компаній, що надають вам юридичні, аудиторські, консультаційні, охоронні послуги, що займаються установкою, адаптацією і підтриманням різного програмного забезпечення і т. п. Доцільно відбирати спеціальне розроблені письмові зобов'язання про нерозголошення комерційної таємниці

Перелік відомостей, що становлять комерційну таємницю, і саме «Положення» - це документи, що вимагають постійного коректування за допомогою відповідних наказів директора, в залежності від змін в чинному законодавстві, обрання підприємством нових видів діяльності, виникнення нових загроз його бізнесу та зміни тактики протиправної діяльності різного роду недоброзичливців.

Надійного забезпечення збереження своєї комерційної таємниці можна досягти тільки за умови комплексного використання на підприємстві всіх елементів системи економічної безпеки, а саме:

- комп'ютерна безпека;
- технічна безпека (в тому числі безпеки зв'язку);
- безпека господарсько-договірної діяльності;
- безпека ділових зустрічей, переговорів;
- масові заходи, рекламні компанії;
- внутрішня безпека;
- конфіденційне діловодство;
- пропускний та внутрішній режим.

1.2.5 Застосування технічних засобів охорони

У загальному випадку система безпеки будь-якого об'єкта являє собою сукупність інженерно-технічних засобів охорони, обслуговуючого персоналу (служби реагування) і організаційних заходів. Далі, говорячи про систему безпеки

об'єкта, ми матимемо на увазі тільки одну її складову - інженерно-технічні засоби охорони.

У свою чергу інженерно-технічні засоби охорони (ІТЗО) діляться на технічні засоби охорони (ТЗО) і засоби технічної укріпленості та інженерні споруди.

До технічних засобів охорони відносяться:

– система охоронної та тривожної сигналізації (СОТС);

– система пожежної сигналізації (СПС);

– система контролю і управління доступом (СКУД);

– система охоронного телебачення (СОТ);

– система безперебійного та резервного електроживлення (СБП);

Системи, що входять в ІТСО, можуть об'єднуватися (інтегруватися) в будь-якому поєднанні між собою в єдиний комплекс (КІТС) за допомогою системи збору і обробки інформації (СЗОІ) з центральним пультом управління (ЦПУ) об'єднаних систем.

Крім перерахованих вище систем до складу КІТС можуть входити:

– система оповіщення про пожежу та управління евакуацією людей (СО);

– система управління димовидаленням (СУД);

– автоматичні установки пожежогасіння (АУПГ).

Для більшої оптимізації при побудові системи захисту від інсайду застосовано обладнання різних виробників, що робить систему гнучкою та збільшує вірогідність збоїв та вимкнення обладнання.

Система контролю і управління доступом (СКУД) - сукупність сумісних між собою апаратних і програмних засобів, спрямованих на обмеження та реєстрацію доступу людей, транспорту та інших об'єктів до (з) приміщення, будівлі, зони і території.

Ідентифікатор користувача - це деякий пристрій або ознака, за якою визначається користувач. Ідентифікаторами можуть бути магнітні картки,

безконтактні проксіміті-карти, брелоки Touch Memory, різні радіобрелоки, зображення райдужної оболонки ока, відбиток пальця, відбиток долоні і багато інших фізичних ознаки. Кожен ідентифікатор характеризуються певним унікальним двійковим кодом. У системі кожним кодом ставиться у відповідність інформація про права та привілеї власника ідентифікатора.

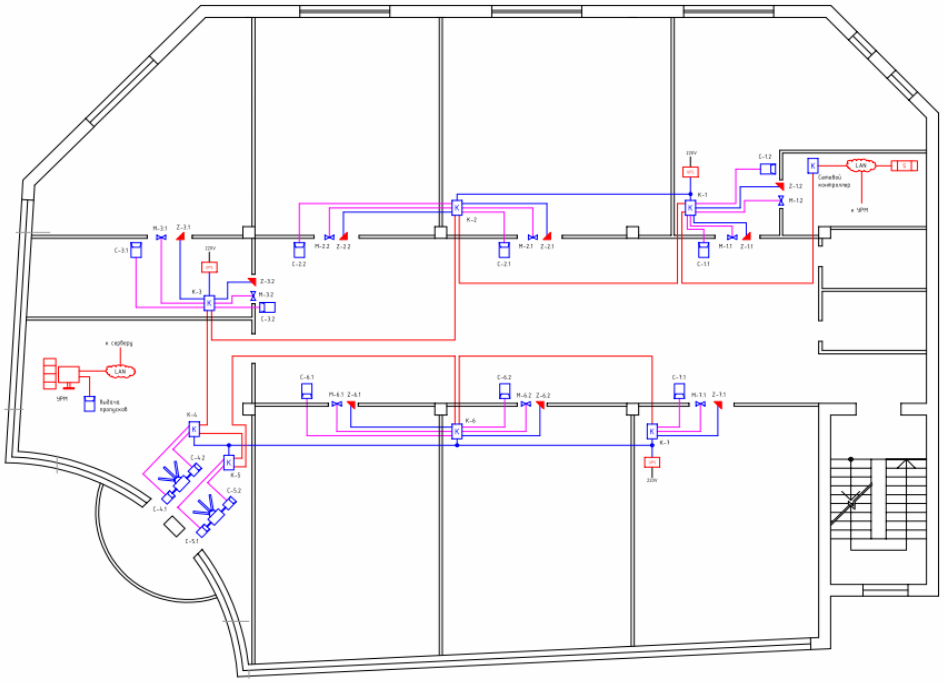


Рисунок 1.7 – Схема розташування системи контролю доступу

Для ефективного використання системи відеоспостереження в офісі не обходимо визначити, коли і в яких ситуаціях система буде вести запис на сервер відеоспостереження або на відеореєстратор. Якщо протягом робочого дня ситуація зрозуміла - система постійно пише, то при використанні її в неробочий час можливі варіанти.

Припустимо, що підприємство не працює з 18.00 по 09.00. Змоделюємо ситуацію, коли в першому випадку система пише постійно, тобто протягом 15-ти

годин. У такому випадку параметр% руху складає 100%. Другий випадок - запис по детектору руху камери. У такому випадку, якщо час знаходження порушника на території становило 30 хвилин, обладнання працювало 3,4% від першого варіанту. На рис. 1.8 приведена схема розміщення відеокамер на планах офісу. При цьому в розрахунку будуть брати участь тільки камери, встановлені внутр. Приміщень у кількості рівному 4.

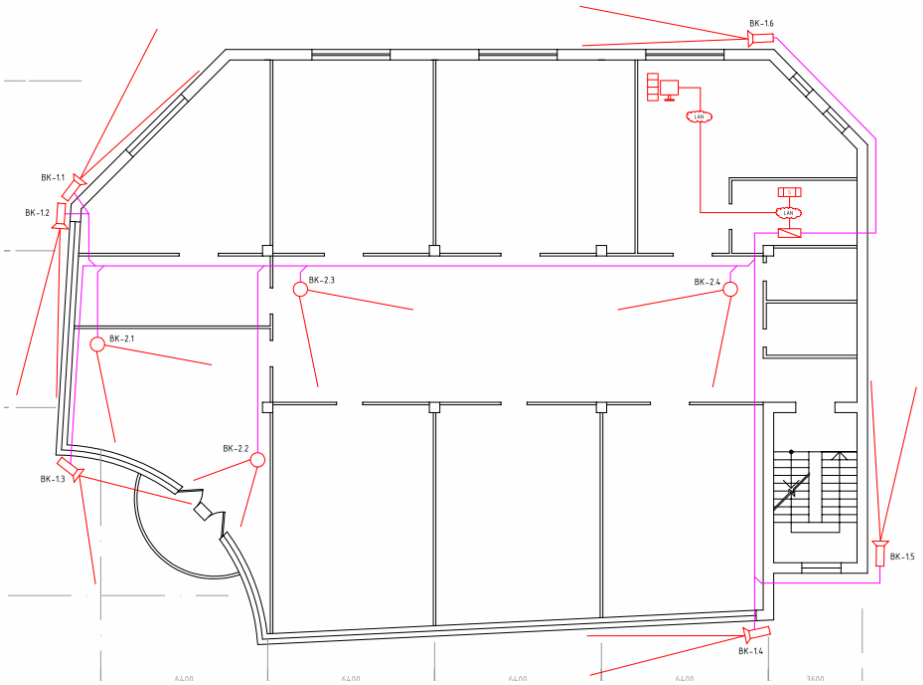


Рисунок 1.8 – Впровадження системи відеоспостереження

1.2.6 Впровадження систем протидії витокам (DLP-систем)

При виборі конкретного рішення необхідно, щоб воно відповідало підходу компанії до захисту інформації. Умовно всі DLP-системи можна розділити на активних, пасивних і комбінованих

1. Активні DLP-системи - це блокування просочування конфіденційної

інформації в режимі реального часу.

Дані системи дозволяють контролювати переміщення конфіденційної інформації по всіх основних каналах комунікації: усередині ЛВС (наприклад, між видаленими підрозділами), через Інтернет, а також на знімні носії, принтери і тому подібне залежно від налагоджених політик такі системи можуть працювати в режимі як блокування, так і моніторингу. Дані системи прийшли до нас з-за кордону, де дуже добре працює законодавство, що оберігає таємницю приватного життя. Тому в таких систем, як правило, відсутній повноцінний архів (зберігаються не всі електронні повідомлення, а лише ті, які порушили політику безпеки компанії), і не можна відновити все листування співробітників при розслідуванні.

Для вчення рядових користувачів роботі з конфіденційними даними у деяких виробників активних DLP-систем закладена можливість повідомлення відправника з проханням підтвердити відправку документа. В цьому випадку співробітник усвідомлює, що вся відповідальність за пересилку конфіденційної інформації ляже на нього.

2. Пасивні DLP-системи — це розслідування інцидентів, що сталися. Дані системи не уміють блокувати просочування інформації, але здатні надати вичерпні відомості про джерело і канали витоку.

Цей тип систем почав розвиватися в Росії як відповідь на потребу першого підходу до інформаційної безпеки, при якому знайти порушників важливіше, ніж запобігти просочуванню конфіденційної інформації. Такі системи складаються з перехоплювачів сніфферов, що копіюють всі електронні повідомлення, що відправляються по основних каналах комунікації: корпоративною і веб-серверу-пошті, соціальним мережам, IM, FTP, принтерам і usb-носіям.

Копії повідомлень зберігаються в архіві. Перед архівацією електронного повідомлення система перевіряє його на відповідність політику ІБ компанії і в разі

невідповідності політиці автоматично оповіщає офіцера безпеки.

3. Потреба в комбінованих DLP-системах виникає при одночасній необхідності архівації всіх електронних повідомлень для подальшого розслідування і можливості блокування витоку конфіденційних даних через основні канали комунікацій. Такі системи починають з'являтися на ринку, але реалізують бажаний «повний комбінований» функціонал лише частково. На сьогоднішній день отримати повноцінну комбіновану DLP-систему можна шляхом інтеграції декількох продуктів.

Основні переваги DLP-системи перед традиційними засобами захисту інформації:

– розслідування інцидентів, пов'язаних з витоками КІ;

– здійснення контролю над всіма каналами передачі конфіденційної інформації в електронному вигляді (включаючи локальні і мережеві способи), регулярно використовуваними в бізнесі-діяльності компанії;

– виявлення інформації, що захищається саме по її вмісту (незалежно від формату зберігання, каналів передачі, грифів і мови);

– можливість блокування витоків (призупинення відправки електронних повідомлень або запису на usb-накопичувачі, якщо ці дії суперечать прийнятій в компанії політиці безпеки);

– автоматизація обробки потоків інформації згідно зі встановленими політиками безпеки (впровадження системи не вимагає розширення штату служби безпеці).

Застосування DLP-систем рекомендується з метою:

– забезпечення безпеки конфіденційної інформації, оброблюваної в Компанії;

– зниження витрат і підвищення ефективності розслідування інцидентів порушення інформаційної та економічної безпеки;

– зниження ризику прямих і непрямих фінансових втрат внаслідок витоку інформації обмеженого доступу (персональні дані 2, таємниця зв`язку 3, банківська таємниця 4 і т. п.).

На ринку представлено багато рішень щодо запобігання витоку конфіденційної інформації. Наведемо основні програмні продукти, які використовуються з метою протидії витокам.

Таблиця 1.6 - Функціонал ПЗ щодо захисту від витоків інформації

	Authentica ARM Platform	InfoWatch Enterprise Solution	Onigma Platform	PC Acme	Verdasys Digital Guardian
Контроль над поштовим трафіком	Так	Так	Так	Ні	Так
Контроль над веб-трафіком	Так	Так	Так	Ні	Так
Контроль над робочими станціями	Так	Так	Так	Так	Так
Комплексність	Так	Так	Так	Ні	Так
Створення архіву корпоративної кореспонденції	Ні	Так	Ні	Ні	Ні
Вибір між програмною та апаратною реалізацією деяких модулів	Ні	Так	Ні	Ні	Ні
Наявність широкого спектру супровідних та консалтингових послуг	Так	Так	Ні	Ні	Так

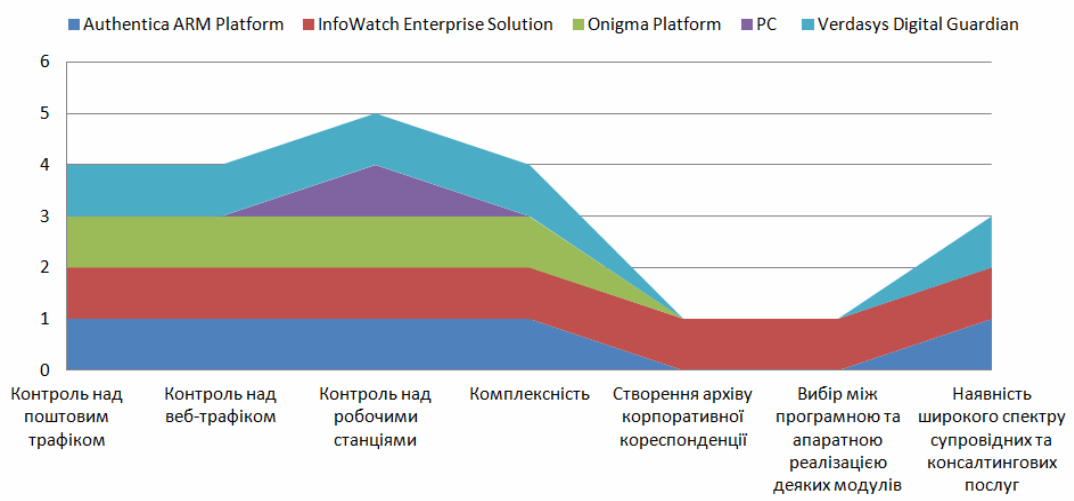


Рисунок 1.9 – Порівняння DLP-систем за ключовими параметрами

2 ОХОРОНА ПРАЦІ

Застосування інформаційних технологій безумовно передбачає використання комп'ютерної техніки. Головна складова цієї техніки, з якою безпосередньо контактує користувач, – це персональний комп'ютер (ПК).

Загальний аналіз умов праці під час роботи з комп'ютерною технікою.

Інтенсивна робота з ПК є причиною виникнення багатьох захворювань Причина відхилень у здоров'ї користувача – переважно недостатнє дотримання принципів ергономіки, неправильна організація робочого місця та санітарно-гігієнічних вимог до умов праці. Все це призводить до виникнення низки захворювань: порушення зору; кістково-м'язових порушень; захворювань шкіри; порушень, пов'язаних зі стресовими ситуаціями та нервово-емоційним навантаженням. З огляду масовість застосування ПК, ця проблема є дуже важливою та актуальною.

Гігієнічні вимоги до виробничого середовища.

Для створення безпечних умов праці розроблені нормативи, які стосуються обладнання приміщень з комп'ютерною технікою, організації робочих місць з ПК, режиму роботи за ПК.

Вимоги до приміщення з розташування робочих місць з ПК.

Згідно з ДСанПіН 3.3.2-007-98 „Державними санітарними правилами і роботи з візуальними дисплейними терміналами електронно-обчислювальних машин", площа приміщення на одне робоче місце користувача ПК повинна становити 6 м^2, а об'єм – не менше 20 м^3. Не дозволяється розміщувати кабінети обчислювальної техніки у підвальних та цокольних поверхах.

Покриття підлоги повинно бути матовим з коефіцієнтом відбиття 0,3–0,5. Поверхня підлоги має бути рівною, неслизькою, з антистатичними властивостями.

Для внутрішнього оздоблення приміщень з ПК треба використовувати дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі 0,7–0,8; для стін 0,5–0,6.

Заборонено застосовувати для оздоблення інтер'єру приміщень з ПК класів полімерні матеріали (деревинно-стружкові плити, шпалери, які можна мити, рулонні синтетичні матеріали, шаруватий паперовий пластик тощо), які виділяють у повітря шкідливі хімічні речовини, що перевищують

Мікроклімат.

Сукупність таких показників виробничого середовища, як температура повітря (°С); відносна вологість (%); швидкість руху повітря (м/с); інтенсивність теплового випромінювання (Вт/м^2, ккал/м^2 год); барометричний тиск (мм рт.ст.), називають метеорологічними умовами, або мікрокліматом.

Для забезпечення нормальних метеорологічних умов у виробничому середовищі з підвищеним виділенням тепла застосовують:

- вентиляцію природну або механічну.
- теплоізоляці*ю* нагрітого обладнання. Поверхні обладнання, що нагріваються, теплоізолюють так, щоб їхня температура не перевищувала +45 °С;
- екранування джерел теплового випромінювання. Обладнання, яке випромінює тепло, відокремлюють від робочої зони екранами. Екрани для захисту від теплового випромінювання поділяють на тепловідбивні і теплопоглинальні;

Все обладнання, що виділяє тепло, розміщують в одному приміщенні;

Шум.

Для захисту від шуму вживають такі заходи:

- Зменшення шуму в джерелі виникнення досягають шляхом його конструктивних змін: заміна металевих деталей на пластмасові;
- Звукоізоляція. Її суть полягає в тому, що найбільша частина звукової енергії, яка падає на звукоізолювальна засоби, відбивається. До

звукоізолювальних заходів належать огородження, стіни, перегородки, спеціальні звукоізолювальні кожухи.

- Архітектурно-планувальні заходи. Найшумніші виробництва рекомендують компонувати в окремі комплекси із забезпеченням розривів між найближчими сусідами.
- Заходи індивідуального захисту. Використання протишумних навушників внутрішніх, що вкладають у вухо, і зовнішніх, які закривають вухо повністю; протишумних касок, спеціального протишумного одягу, які ізолюють тіло і поглинають звук.

Дія вібрації на організм людини та захист від вібрації.

Вібрацію людина сприймає як трясіння. Часто вібрація супроводжується шумом, який чує людина.

Заходами захисту від вібрації є:

- зменшення вібрації в джерелі виникнення, що досягають шляхом його конструктивних змін;
- зменшення вібрації на шляху поширення, що досягають віброізоляціїєю, вібропоглинанням або віброгасінням.
- індивідуальний захист за допомогою спеціального одягу.

Електромагнітне випромінювання і його характеристики.

Захист передбачає обмежене перебування людини в електромагнітному полі (ЕМП). Допустимий час перебування людини в ЕМП залежить від інтенсивності опромінення або напруженості ЕМП.

Зменшення потужності випромінювання безпосередньо в джерелі досягають використанням спеціальних пристроїв – поглиначів потужності (еквівалент антени і навантаження), які повністю поглинають або знижують енергію електромагнітного випромінювального, що передається на шляху від генератора до випромінюючого пристрою. Екранування джерел випромінювання

використовують для зменшення інтенсивності ЕМП на робочому місці. Для цього застосовують заземлені екрани з металевих листів або сіток у вигляді замкнутих камер, кожухів.

Електробезпека.

До головних способів захисту від ураження електричним струмом у разі дотику людини до частин обладнання, що проводять струм, належать: ізоляція, використання малих напруг, електричне розділення мереж, обгороджувальні пристрої, попереджувальна сигналізація, блокування, засоби захисту, запобіжні пристосування.

Вимоги до організації робочого місця працівника.

Обладнання та організація робочих місць користувачів ПК мають забезпечувати відповідність конструкцій усіх елементів робочого місця та їхнього взаємного розташування ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності. У разі розташування елементів робочого місця користувача ПК треба враховувати: робочу позу користувача, простір для розміщення користувача, можливість огляду елементів робочого місця, можливість ведення записів, розміщення документації і матеріалів, які використовує користувач.

Конструкція робочого місця користувача ПК повинна забезпечити підтримання оптимальної робочої пози. Робочі місця з ПК треба так розташовувати щодо вікон, щоб природне світло падало збоку переважно ліворуч. Робочі місця з ПК повинні бути розташовані від стіни з вікнами на відстані не менше 1,5 м, від інших стін – на відстані не менше ніж 1 м. У разі розміщенні робочого місця поряд з вікном кут між екраном монітора площиною вікна повинен становити не менше 90° (для уникнення відблисків), частину вікна, що прилягає, потрібно зашторити. Недопустиме розташування ПК, за якого працівник повернений обличчям або спиною до вікон кімнати або до задньої частини ПК, в яку монтують вентилятори.

У разі розміщення робочих столів з ПК треба дотримуватись таких відстаней: між бічними поверхнями ПК – 1,2 м, від задньої поверхні одного ПК до екрана іншого ПК – 2,5 м.

Монітор повинен бути встановлений так щоб верхній край екрана перебував на рівні очей. Екран монітора ПК повинен бути на оптимальній відстані від очей користувача, що становить 600–700 мм, але не ближче ніж 600 мм з урахуванням розміру літерно-цифрових знаків і символів. Для забезпечення точного та швидкого зчитування інформації в зоні найліпшого бачення площина екрана монітора повинна бути перпендикулярною до нормальної лінії зору. Розташування екрана монітора ПК має забезпечувати зручність зорового спостереження у вертикальній площині під кутом 30° до нормальної лінії погляду користувача.

Клавіатура повинна бути розташована так, щоб на ній можна було зручно працювати двома руками. Клавіатуру треба розміщати на поверхні столу на відстані 100–300 мм від краю. Кут нахилу клавіатури до столу повинен бути в межах від 5° до 15°, зап’ястя та долоні рук повинні бути розташовувані горизонтально до площини столу.

Конструкція робочого стола повинна забезпечувати можливість оптимального розміщення на робочій поверхні обладнання з урахуванням його кількості та конструктивних особливостей (розмір монітора, клавіатури, принтера, ПК тощо) і документів, а також враховувати характер виконуваної роботи.

Висота робочої поверхні столу з ПК повинна бути в межах 680–800 мм, а ширина і глибина – забезпечувати можливість виконання операцій у зоні досяжності моторного поля (рекомендовані розміри: 600–1400 мм, глибина – 800–1000 мм). Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною – не менше 500 мм, глибиною (на рівні колін) – не менше 450 мм, на рівні простягнутої ноги – не менше 650 мм.

Ноги не повинні бути витягнені під час сидіння далеко вперед, тому що в такому разі м’язи будуть надто напружені; положення „нога на ногу” не рекомендоване, тому що підвищується тиск на сідничний нерв і порушується кровообіг ніг.

Робочий стілець має бути підйомно-поворотним, регульованим за висотою, з кутом нахилу сидіння та спинки, поверхня сидіння має бути плоскою, передній край – заокругленим. Регулювання за кожним із параметрів повинне бути незалежне, а фіксування легким і надійним. Висота поверхні сидіння має бути регульована в межах 400–500 мм, а ширина і глибина становити не менше 400 мм. Кут нахилу сидіння – до 15° вперед і до 5° назад. Висота спинки стільця має становити 300±20 мм, ширина – не менше 380 мм. Кут нахилу спинки має бути регульований у межах 1–30° від вертикального положення, відстань від спинки до переднього краю сидіння – у межах 260–400 мм.

Для зниження статичного напруження м’язів верхніх кінцівок треба використовувати стаціонарні або змінні підлокітники завдовжки не менше 250 мм, завширшки – 50–70 мм, регульовані за висотою над сидінням у межах 230–260 мм і відстанню між підлокітниками у межах 350–500 мм.

Поверхня сидіння і спинки стільця має бути напівм’якою з нековзним повітронепроникним покриттям, що легко чистити і яке не електризує.

Робоче місце має бути обладнане підставкою для ніг шириною до 300 мм, глибиною – не менше 400 мм, що регульована за висотою в межах до 150 мм і за кутом нахилу опорної поверхні підставки – до 20°. Підставка повинна мати рифлену поверхню і бортик по передньому краю заввишки 10 мм.

Вимоги до режимів праці і відпочинку під час роботи з ПК.

Режими праці й відпочинку у разі роботи з ПК розробляють з урахуванням характеру трудової діяльності, напруженості і важкості праці диференційовано до

кожної професії. Залежно від характеру праці визначають такі внутрішньозмінні режими праці та відпочинку:

У всіх випадках, коли виробничі обставини не дають змоги застосувати регламентовані перерви, тривалість безперервної роботи з ПК не повинна перевищувати 4 год.

Щоб зменшити негативний вплив монотонності на працівника треба чергувати деякі операції, наприклад, уведення тексту за допомогою клавіатури та редагування тексту тощо.

Для зниження нервово-емоційного напруження, втоми зорового аналізатора, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільно деякі перерви використовувати для виконання комплексу вправ.

Пожежна безпека.

Джерелами запалювання на підприємствах можуть бути: відкрите полум'я, невідповідність або несправність електрообладнання, іскри від удару і тертя деталей машин і обладнання, самозайманння, статична електрика, розряд блискавки та ін.

Пожежна небезпека електрообладнання, електронних приладів, радіо-електронної апаратури, апаратури керування, електроприймачів пов'язана з використанням гуми, пластмас, лаків, олій.

Для організації пожежної безпеки всі приміщення повинні бути забезпечені первинними засобами пожежогасіння: пожежним водопостачанням (пожежні крани ПК), пожежні щити з набором пожежного інструменту, вуглекислотними або порошковими вогнегасниками. У випадку виникнення пожежі необхідно відключити електроживлення, викликати по телефону 101 пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації і пр.

ВИСНОВОК

Отримані при виконанні бакалаврській роботи результати можна використовувати в діяльності державних та комерційних підприємств всіх форм власності. Проведення першочергових заходів щодо захисту комерційної таємниці та впровадження конфіденційного документообігу суттєво знизять інформаційні ризики підприємства, а застосування методики оцінки кадрових ризиків та інструктажі персоналу допоможуть своєчасно виявити та згодом запобігти роботі внутрішнього порушника. У бакалаврській роботі представлено методологію захисту від внутрішнього порушника.

Результати роботи такі:

1. Розглянуто формування системи захисту підприємства з позиції проблематики інсайдерства.

2. Проведено дослідження напрямку комерційної таємниці підприємства, а саме, дано визначення, відмінні ознаки, види відповідальності, представлено алгоритм формування положення про комерційну таємницю.

3. Розглянуто роботу з документацією як основний напрям СЗІ згідно завдання, тому проведено детальне дослідження методів роботи з конфіденційною інформацією на шляху всього “життєвого” циклу.

4. В рамках формування методології захисту застосовано різні елементи захисту – технічні засоби охорони, системи протидії витокам, USB-накопичувачі з криптозахистом тощо.

5. З позиції виявлення потенційних порушників на ранніх стадіях застосовано методику оцінки кадрових ризиків.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дворский М.Н.,Палатченко С.Н. Техническая безопасность объектов предпринимательства, 1 том, 2006.–17 с.

2. А. Лыткин. IP - видеонаблюдение. Наглядное пособие // Издательство “Авторская книга”, 2011. – 200 стр.

3. Астахова Л.В., Землянская О.О., Методика оценки кадрових уязвимостей информационной безопасности организации на этапе приема сотрудника на работу // Вестник Южно-Уральского государственного университета, №1(7), 2013, с.53-58

4. А. Маркевич. Расчет видеоархива и сети [електронний ресурс]. – Режим доступу: http://markevich.by/raschet-videoarxiva-propusknoj-sposobnosti-seti

5. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008.-320 с.

6. Лянной Г., Положение о коммерческой тайне, дань моде или средство защиты предприятия / Журнал Best of Security – Лучшее о безопасности, №2 (февраль), 2007

7. С.В. Стайкуца, О.М.Плотна // Дослідження методів та рішень при впровадженні системи захисту інформації на прикладі медичної установи // Матеріали третьої міжнародної наукова-практичної конференції молодих вчених “Інфокомунікації – сучасність та майбутнє”, ОНАЗ ім. О.С.Попова – Одеса, 20-23 жовтня 2013 р.

8. Стайкуца С.В. Основні визначення комерційної таємниці підприємства / Стайкуца С.В. //Конспект лекцій з курсу “Організаційне забезпечення технічного захисту інформації”, ОНАЗ ім.О.С.Попова, 2012

9. Інструкція про порядок обліку, зберігання і використання документів,

справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави". Затверджена Постановою Кабінету Міністрів України від 27листопада 1998р. № 1893.

10. Довідник кваліфікаційних характеристик професії працівників. Випуск 42. Затверджено та введено в дію наказом Міністерства промислової політики України від 22 березня 2007 року №120.

11. Примірне положення про архівні підрозділи підприємства, установи та організації, заснованих на приватній формі власності, об'єднання громадян, релігійної організації. Затверджено наказом Державного комітету архівів України від 5 червня 2002 року № 42.

12. Правила роботи архівних підрозділів органів державної влади, місцевого самоврядування, підприємств, установ і організацій. Затверджені наказом Державного Комітету архівів України від 16 березня 2001 року № 16.

13. Мишина Л.А. Делопроизводство: Учебно-методическое пособие для студентов ИПП всех специальностей Минск, 2004 - 102 с.

14. Хвалей М.К. Делопроизводство и деловая (торговая) корреспонденция: Учеб. пособие. — Мн.: БГЭУ, 2002. — 253 с.

15. UAC. Українська архітектурна компанія. Архівна обробка документів [Електронний ресурс]. – Режим доступу: http: // иас - archive.com.ua.

16. ....Уничтожить нельзя сохранить... Как выбрать уничтожитель документов // "BEST OF SECURITY". - К, 2006. - №10.

17. Организация службы безопасности предприятия [Електронний ресурс]. – Режим доступу: http://www.bre.ru/secu- rity/83.html.

18. Основные критерии выбора уничтожителя документов [Електронний ресурс]. – Режим доступу: http://az.hiota zh.com

19. Бійтеся данайців, що дари підносять, або Хто такі інсайдери? [Електронний ресурс]. — Режим доступу: http://arhiv-tatey.pp.ua/index.php.

20. Эффективность применения DLP-системы[електронний ресурс]. – 2014. Режим доступу: http://habrahabr.ru/sandbox/77112/.

21. Сравнение систем защиты от утечек (DLP) [Електронний ресурс]. – Режим доступу: http://www.anti-malware.ru/comparisons

22. Основные критерии выбора уничтожителя документов [Електронний ресурс]. - Режим доступу: http://az.hio-tazh.com

23. Конфіденційне діловодство як важлива складова системи захисту конфіденційної інформації, що є власністю юридичних осіб [Електронний ресурс]. - Режим доступу: http://www.yurradnik.com.ua/stride/ur/index.php

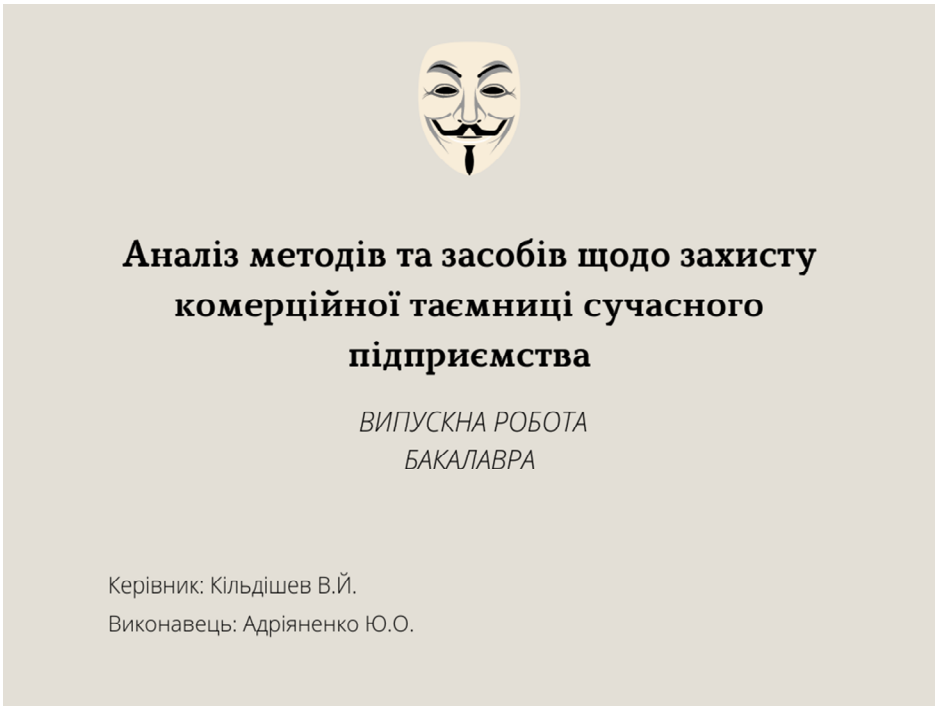
24. Мельников А. М. Организация защиты коммерческой тайны [Електронний ресурс] / А. М. Мельников, О. А. Коваленко – Режим доступу до ресурсу: https://studbooks.net/57071/ekonomika

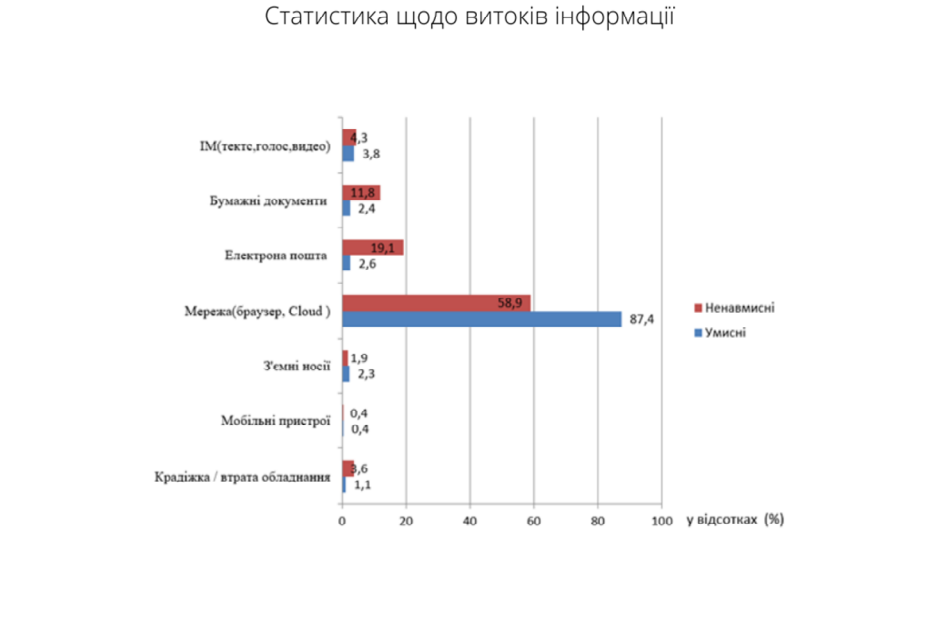
25. Мероприятия по обеспечению сохранности коммерческой тайны ООО «Астра-ком» [Електронний ресурс] – Режим доступу до ресурсу: http://refleader.ru/jgeqasmerbew.html.

26. Колобов Л. Комерційна таємниця та питання захисту комерційної таємниці / Л. Колобов, І. Колеснікова. // Цивільне право і процес. – 2016. – №5. – С. 8–13.

Додаток А

КОПІЇ СЛАЙДІВ МУЛЬТИМЕДІЙНОЇ ПРЕЗЕНТАЦІЇ





2

Базові визначення

Інсайдери

це авторизовані користувачі, які мають законний доступ до конфіденційної інформації і вони можуть знати уразливі місця розгорнутих систем і бізнес-процесів.

3

Визначення та класифікація правопорушень

Інсайдерська діяльність

спрямовані дії мотивованих суб'єктів, які мають легітимний доступ до інформаційних активів та навички для здобуття цінної інформації, знають уразливі місця інформаційних систем і бізнес-процесів для завдання матеріальних збитків та/або репутаційних втрат організації.

4

Класифікація інсайдерів

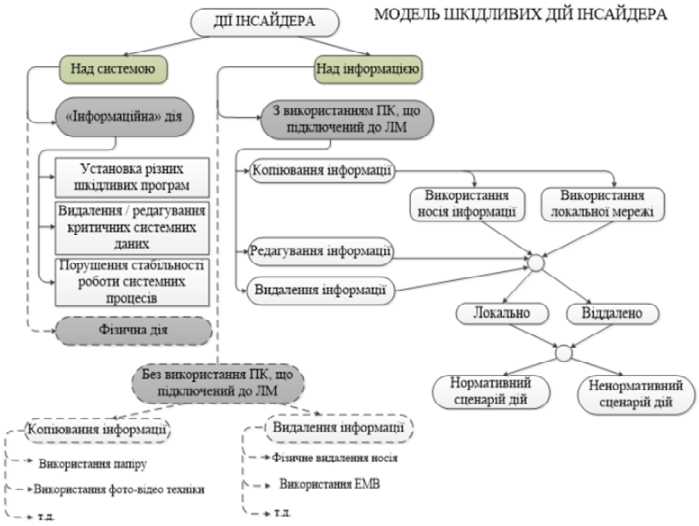
Тип	Намір	Користь	Постановка завдання	Дії при неможливості
Недбалий	ні	ні	ні	повідомлення
Маніпульований	ні	ні	ні	повідомлення
Скривджений	так	ні	сам	відмова
Нелояльний	так	ні	сам	імітація
Сумісник	так	так	сам/ззовні	відмова /імітація/злам
Впроваджений	так	так	ззовні	злам

Базова класифікація інсайдерів, 6 типів

Альтернативна класифікація інсайдерів

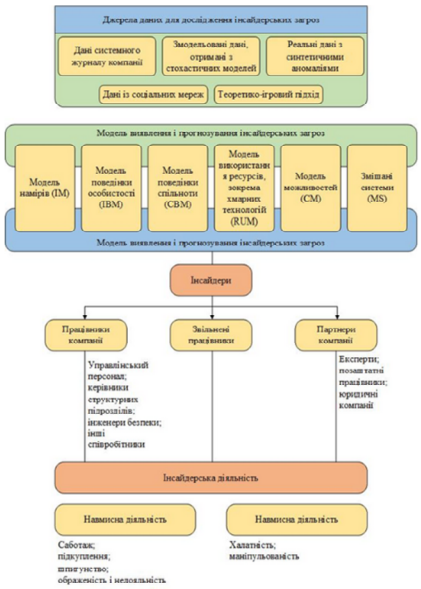
5

Модель шкідливих дій інсайдера



6

Глобальна екосистема інсайдерської діяльності



Організаційно-технічні заходи щодо забезпечення збереження комерційної таємниці на підприємстві

Використання методики оцінки кадрових ризиків

Анкета для оцінки кандидата

Категорія співробітника			Досліджуваний блок	Питання. Інший показник оцінки
I	II	III		
✓	✓	✓	Зайва балакучість	Прохання розповісти про вчорашній день
✓	✓			«Ви товариська людина?»
✓				У ході співбесіди
✓	✓	✓	Прагнення помститися керівництву або колезі по роботі	«Ви легко вибачаєте людей?»
✓	✓			Думка про попереднє місце роботи
✓	✓	✓	Схильність до розваг, пияцтву, наркотикам	«Чим ви захоплюєтеся?»
✓	✓			«Як Ви ставитеся до проведення вільного часу у великій галасливій компанії?»
✓	✓	✓	Наявність шкідливих звичок	«Чи є у Вас шкідливі звички?»
✓	✓	✓	Уважність	Психологічне тестування «Коректурна проба» (Тест Бурдона)
✓	✓	✓	Схильність маніпуляціям (вплив з боку зловмисника)	«Наскільки складно змінити Ваше думку?»
✓	✓			Тест «Піддаються ми маніпуляції?» З книги Кіри Буреніної
✓				(Спроба маніпулювати)
✓	✓	✓	Некваліфіковане виконання операцій	Провокація на розголошення КІ (Сценарій для кожної посади продумується індивідуально)
✓	✓	✓		«Чи є у вашій роботі інформація, поширення якої обмежено?»
✓	✓	✓	Сторінка в соціальній мережі	Аналіз змісту анкети, повідомлень, фото- і відеоматеріалу
✓	✓			Список цікавих груп, сторінок, на які підписаний користувач
✓				Рівень конфіденційності сторінки
✓	✓		Звернення на попереднє місце роботи	Бесіда з керівником, співробітниками, які мають можливість дати характеристику співробітникам (секретар, вахтер)
✓			Запит за особистими даними в пошукових системах	Виявлена інформація інтерпретується індивідуально в кожному випадку

$$P = \frac{\sum_{i=1}^{N} p_i}{4N}$$

де
P – коефіцієнт вразливості кандидата
N - кількість виставлених оцінок (у тому числі оцінки «0 балів»);
pi - кількість балів за i-ту відповідь;
i - порядковий номер відповіді.

Використання технічних засобів охорони

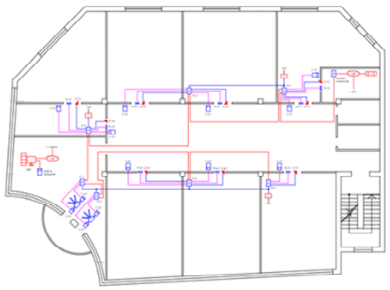
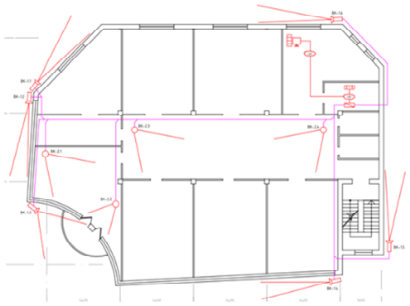


Схема розташування системи контролю доступу



Розташування елементів системи відеоспостереження

Алгоритм формування "Положення про комерційну таємницю"

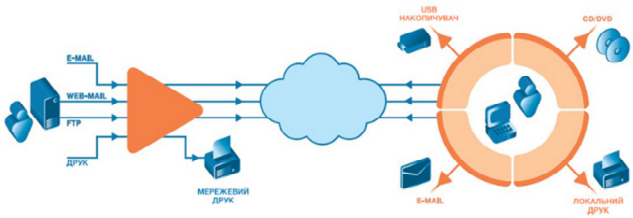
БАЗОВИЙ АЛГОРИТМ

- РОЗРОБКА ПОЛОЖЕННЯ ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ (КТ)
- РОЗРОБКА ІНСТРУКЦІЙ ЩОДО ДОТРИМАННЯ СПІВРОБІТНИКАМИ РЕЖИМУ НЕРАЗГОЛОШЕННЯ КТ
- ВКЛЮЧЕННЯ ДО СТАТУТУ ПІДПРИЄМСТВА РОЗДІЛІВ, ЩО РЕГЛАМЕНТУЮТЬ ЗАХИСТ КТ
- РОЗРОБКА УГОДИ ПРО НЕРАЗГОЛОШЕННЯ КТ. УКЛАДАЄТЬСЯ З ОСОБАМИ, ЯКІ МАЮТЬ ДОСТУП ДО КОМЕРЦІЙНОЇ ТАЄМНИЦІ

11

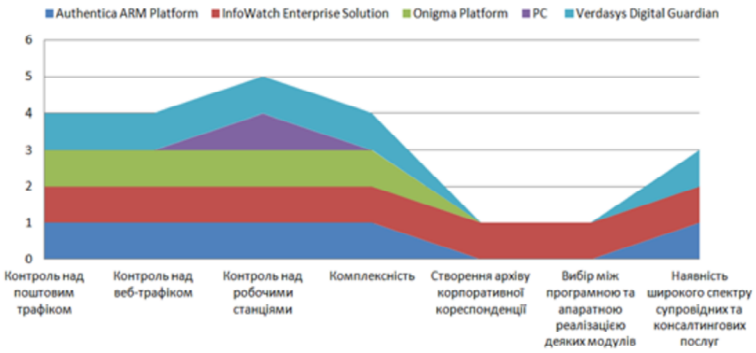
Використання DLP-систем

Data Leak/Loss/Leakage Prevention (DLP) – технології запобігання витоків конфіденційної інформації, що є власністю організації, за межі її інформаційної системи, а також комплекс технічних засобів (програмних або програмно-апаратних) для запобігання витокам.



12

Порівняння DLP-систем за ключовими параметрами



ДЯКУЮ ЗА УВАГУ!

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015395529

Дата перевірки:
02.06.2023 15:07:57 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
02.06.2023 15:11:04 EEST

ID користувача:
100011688

Назва документа: 2БКС-27_Олексій_Андріяненко

Кількість сторінок: 49 Кількість слів: 8372 Кількість символів: 65743 Розмір файлу: 882.67 KB ID файлу: 1015059737

37.7%
Схожість

Найбільша схожість: 17.9% з Інтернет-джерелом (https://csecurity.kubg.edu.ua/index.php/journal/article/download/347...

37.7% Джерела з Інтернету | 684 ..... Сторінка 51

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 7

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Андріяненко Олексія Юрійовича

(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

«Аналіз методів та засобів щодо захисту комерційної таємниці сучасного підприємства»

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 відмінно

Оцінка графічної (презентаційної) частини відмінно

Загальна оцінка відмінно

Прізвище, ім'я та по батькові рецензента Царьов Роман Юрійович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку, старший викладач кафедри комп'ютерної інженерії та інформаційних систем

«16» червня 2023 р. (підпис) Царьов Р. Ю. (прізвище та ініціали рецензента)

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ
КАДРІВ ДУІТЗ

ВІДДІЛ КАДРІВ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника про кваліфікаційну роботу бакалавра

Андріяненко Олексія Юрійовича

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

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

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи

«Аналіз методів та засобів щодо захисту комерційної таємниці сучасного підприємства»

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 відмінно

Оцінка графічної (презентаційної) частини відмінно

Загальна оцінка відмінно

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» 06 2023 р. _____ Кільдішев В.И.

(підпис) (прізвище та ініціали керівника)

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

Ми, що нижче підписалися,

Андріяненко Олексій Юрійович
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:

«Аналіз методів та засобів щодо захисту комерційної таємниці сучасного підприємства» (автор роботи – Андріяненко О.Ю., 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 _____ / Андріяненко О. Ю. /

Керівник _____ / Кільдішев В.Й. /

«15» 06 2023 р.