МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Освітньо-професійна програма «Комп'ютерна інженерія

Спеціальність 123 «Комп'ютерна інженерія»

Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА

БАКАЛАВРА

здобувача освіти денної форми навчання
БКС 27.20.000.00 БКР

Поляков Ілля Дмитрович

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

Освітньо-професійна програма: «Комп'ютерна інженерія»
Спеціальність 123 «Комп'ютерна інженерія»
Група БКС-27

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра на тему:

«Аналіз методів та засобів інформації безпеки українського ІТ-бізнесу»

Проектний матеріал складається з пояснювальної записки на 66 сторінках та мультимедійної презентації на 12 сторінках.

Здобувач освіти _____ (Поляков І.Д.)
Керівник роботи _____ (Харченко Р.Ю.)

Консультанти:
з охорони праці _____ (Чорновол Н.І.)
за дотриманням вимог ЄСКД _____ (Петрашова В.І.)
старший консультант _____ (Кривченко Ю.В.)

До захисту допущений
Завідувач кафедри _____ (Іванова І.В.)
Завідуючий відділенням _____ (Скорнякова О.В)

Захист «26» 06 2023 р. Протокол ДКК № 3
Оцінка ДКК 4 (добре)
Секретар ДКК _____

АНОТАЦІЯ

Розглянуті питання, які пов'язані з інформаційною безпекою українських ІТ-підприємств.

Інформаційна безпека являє собою набір інструментів і методів, використовуваних для захисту цифрової та аналогової інформації. Показано призначення системи управління інформаційною безпекою і роль технічних засобів захисту інформації від інформаційних загроз підприємству. Для створення та ефективної експлуатації системи забезпечення інформаційної безпеки необхідно завжди використовувати вже напрацьовані практики (стандарти, методології) побудови подібних системи забезпечення інформаційної безпеки та реалізовувати їх до систем управління (менеджменту) інформаційною безпекою

Запропоновано до реалізації інноваційні рішення від Microsoft та проаналізовані кібератаки які можуть прийти через постачальників підприємств України в цілях підвищення ефективності виявлення інформаційних сучасних загроз і захисту інформації.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

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.

"_____" _____ 20 ____ р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачу освіти *Полякову Іллї Дмитровичу*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз методів та засобів інформаційної безпеки українського IT-бізнесу*

затверджена наказом по коледжу від "17" 10 2022 р. № 235-АД-ОД

2. Термін здачі студентом кваліфікаційної роботи 16.06.2023 р.

3. Вихідні дані до роботи *1. Identities; 2. Веб-додатки; Conditional-access;MFA; Intune MAM 3. Система захисту веб-сайту; 4. DDoS-атаки; 5. Firewal;l 6. Системи виявлення атак (СВА); 7. Intune MDM; 8. Web Firewall Application; Supply chain attack;*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1.Безпека IT компанії;

2. Політика безпеки українських IT-компаній;

3. Аналіз кібератак на ланцюг поставок

5. Перелік графічного матеріалу (слайдів мультимедійної презентації)

Ризики кібербезпеки; Найважливіші питання щодо IT-ризиків; Система інформаційного контролю I

Принцип дії MFA; Набір правил управління доступом Conditional-access ; Intune (MAM);

Набір правил управління доступом Conditional-access; Intune MDM; Shadow IT Lifecycle

Microsoft Defender для хмарних технологій, Заходи протидії Supply chain attack; Гратчаста структура сайту; Анализ атаки через компанію-підрядника

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

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

7. Дата видачі завдання 01.05.2023

Керівник роботи *Харченко Р.Ю.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз предметної галузі*	5.05.2023	виконав
2.	*Аналіз технічного завдання та пошук літератури*	7.05.2023	виконав
3.	*Складники безпеки ІТ компанії*	9.05.2023	виконав
4.	*Захист конфіденційної інформації в ІТ-компаніях*	11.05.2023	виконав
5.	*Оцінка ІТ ризиків*	13.05.2023	виконав
6.	*Політика інформаційної безпеки ІТ-компанії*	16.05.2023	виконав
7.	*Методи забезпечення інформаційної безпеки*	18.05.2023	виконав
8.	*Кібератаки в Україні 2023: огляд загальної ситуації*	20.05.2023	виконав
9.	*Перевірка конфігурації сервера*	23.05.2023	виконав
10.	*Application: виявлення потенційно небезпечних програм*	25.05.2023	виконав
11.	*Infrastructure: організація безпечної роботи в хмарі*	27.05.2023	виконав
12.	*Network: безпечний доступ до корпоративної мережі*	30.05.2023	виконав
13.	*Supply chain attack*	3.06.2023	виконав
14.	*Приклади кібератак на ланцюг постачання*	5.06.2023	виконав
15.	*Розробка питань з охорони праці*	8.06.2023	виконав
16.	*Оформлення креслень та тексту ПЗ*	10.06.2023	виконав

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27. 20. 000. 00 БКР	Випускна робота бакалавра	66	
А4			БКС 27. 20 000. 00 БКР ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 27. 20 000. 00 БКР		
Розробив		Поляков І.Д.			Аналіз методів та засобів інформаційної безпеки українського ІТ-бізнесу	Літ.	Аркуш 4 / Аркушів
Перевірив		Харченко Р.Ю.				У Д П	
Н. Контр.		Петрашова В.І.				ОТФК ОНТУ, гр. 2БКС-27	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Сучасний етап розвитку суспільства пов'язаний з масштабним використанням інформаційних технологій та створенням єдиного інформаційного простору, в якому інформація зберігається, обробляється та обмінюється. Питання інформаційної безпеки має першочергове значення в усіх сферах суспільної та державної діяльності. У цьому контексті необхідність систем захисту комп'ютерної інформації від несанкціонованого доступу, крадіжки, знищення та інших злочинних і небажаних дій є очевидною. Всі технічні бізнес-процеси піддаються впливу питань безпеки та конфіденційності. Сучасні інструменти безпеки можуть протистояти атакамкіберзлочинців, однак цього недостатньо. Тому підприємства та юридичні особи повинні забезпечити засоби внутрішні політики та поведінкаспівробітників, щоб мінімізувати або значно зменшити ці ризики. За оцінками американських експертів, щорічні збитки від комп'ютерних злочинівстановлять приблизно 35 мільярдів доларів США. Основи системи управління інформаційною безпекою зосереджені на оцінки та управління ризиками. Процес управління ризиками безпеки дозволяє організаціям досягти поєднання відомих прийнятних рівнів ризику та максимальної економічної ефективності. Управління інформаційною безпекою стає можливим завдяки підтримці безпеки інформаційно-комунікаційних систем і мереж за допомогою певних інструментів і засобів контролю.Аналіз інформаційної безпеки є критично важливим для будь-якого бізнесу, оскільки він забезпечує синхронізацію системі процесів IT та інформаційної безпеки з урахуванням найкращих світовихпрактик і стандартів для мінімізації бізнес-ризиків.

В Україні інформаційна безпека реалізується шляхом захисту інформації у випадках, коли необхідність захисту інформації визначена законодавством у сфері захисту інформації. Для реалізації захисту інформації створюється Комплексна система захисту інформації (КСЗІ).

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Безпека ІТ компанії

1.1.1 Складники безпеки ІТ компанії

Управління ІТ-бізнесом - це складний процес, що вимагає ретельного, системного підходу та найвищого рівня контролю і безпеки. Чим більша компанія, тим складніша система управління і тим важче встановити процеси звітності та рівні відповідальності; в системі управління ІТ-бізнесом важливу роль відіграють наступні заходи:

- Розробка політик конфіденційності, які повинні бути доведені до відома всіх працівників.
- Підписання договорів про конфіденційність із чіткими вимогами щодо фіксування наслідків витоку інформації.
- Використання ліцензованого програмного забезпечення для роботи із операційними завданнями бізнесу.
- Формування практик зберігання операційних документів у «хмарних середовищах».
- Запровадження електронного документообігу.
- Інші заходи у сфері ІТ, що спрямовані на попередження витоків інформації та хакерських атак на підприємство.

За підтримки ІТ-відділу компанії необхідно сформувати відповідну технічну інфраструктуру для захисту конфіденційності всього документообігу компанії. Тимчасом юридичний відділ та відділ кадрів повинні сформулювати політику поводження з конфіденційною інформацією, правила використання обладнання компанії за межами її території та розробити проекти у год про конфіденційність.

Отже, безпека ІТ компанії це:

- становище найбільш ефективного використання усіх ресурсів для запобігання внутрішніх і зовнішніх загроз та забезпечення стабільного функціонування компанії на теперішній час і в майбутньому;
- захищеність діяльності від негативного впливу зовнішніх та внутрішніх факторів в оточенні, а також можливість оперативного усунення різноманітних «загрожуючих чинників» або швидкого адаптування до існуючих умов, які не відбиваються негативно на діяльності компанії та/або максимально мінімізують всілякі негативні фактори впливу;.
- комплекс заходів, які сприяють підвищенню фінансового потенціалу та забезпечують економічний приріст компанії за умов жорсткої конкуренції та динаміки розвитку ІТ галузі, а також захищають комерційні інтереси від впливу різноманітних негативних процесів і «подразнюючих чинників»;
- сукупність чинників, які забезпечують незалежність, стійкість, здатність до прогресу в умовах дестабілізуючих факторів;
- захищеність цифрового, технічного, технологічного, виробничого та кадрового потенціалу від прямих (активних) або непрямих (пасивних) загроз.

Іншими словами, безпека для ІТ-компаній – це стійкий і динамічний розвиток, що досягається за рахунок використання всіх видів ресурсів і здатності гарантувати їх найбільш ефективне використання для стабільного управління і динамічного розвитку, а також за рахунок запобігання несприятливим внутрішнім і зовнішнім впливам (загрозам).

Майже всі ІТ-компанії на певному етапі свого розвитку та функціонування стикаються з низкою ризиків та загроз, які, якщо їх не усунути, можуть мати непередбачувані наслідки.

1. Фізична безпека ІТ компанії.

Фізична безпека IT компанії Це не означає, що ми або наша команда повинні всюди мати охоронців, але ви неповинні нехтувати, здавалося б, елементарними речами.

Зокрема, але не виключно:

- потрібно подбати про доступ до вашого офісного приміщення. Встановлення навіть найпростіших елементів захисту фізичного доступу (електронні та цифрові замки наприклад) дозволить суттєво мінімізувати потік небажаних гостей, а, у випадку застосування передових технологій взагалі унеможливить присутність у вашому робочому просторі персонажів «я просто спросить».
- Ефективним також буде декілька-рівневий формат доступу до приміщення. Наприклад, попередній контроль та ідентифікація відвідувачів на рецепції та в подальшому безпосередньо при вході до офісного приміщення не буде зайвим.
- Наявність систем постійної відеофіксації простору навколо офісу також створить певні незручності «небажаним гостям» або фейковим клієнтам.
- В окремих випадках доцільно також розглядати присутність так званого фізичного фільтру у вигляді фахівця із забезпечення безпеки.

2. Люди, як фактор ризику.

Більшість власників IT-компаній намагаються сформувати команду з "перевіреного середовища" на старті свого бізнесу або конкретного проекту. Однак з часом так чи інакше виникає потреба в залученні спеціалістів ззовні.

Проте, як незнайомі нам раніше люди так і «перевірені товариші» можуть свідомо чи несвідомо піддавати ризикам стабільне функціонуваннякомпанії.

Важливо розробити та затвердити концепцію діяльності IT-компанії, яка встановлює рівні доступу та обмеження доступу до інформації відповідно до реальних потреб. Особливу увагу варто приділити наданню віддаленого

доступу фахівцям, які займаються окремими проектами та діяльністю компанії в цілому.

При можливості та наявності відповідних ресурсів потрібно здійснювати додаткову спеціальну перевірку співробітників та фахівців, які залучаються до окремих важливих проектів і яким можуть передаватися конфіденційні відомості.

Крім того, офісні приміщення слід зонувати за проектами або професійними напрямками діяльності. Також слід пам'ятати про належну координацію відносин між співзасновниками IT-компанії. Чіткий розподіл прав, обов'язків, межі засобів впливу на діяльність компанії має бутиврегульовано в корпоративному договорі – цей елемент безпекової складової IT-компанії допомагає скоординувати поведінку осіб, які беруть участь в управлінні компанією.

Важливо не ігнорувати таку складову, як навчання команди. Навчання ефективній протидії негативним обставинам та надання конкретних алгоритмів виявлення та боротьби з причинами, що створюють ризики для безпеки IT компанії допоможе підвищити рівень безпеки в IT компанії в цілому.

3. IT безпека IT компанії

IT-персонал часто не замислюється над важливістю безпеки та існуванням вразливостей у мережі та програмному забезпеченні компанії, оскільки вони занадто зосереджені на проектах або просто не мають достатньо часу. Це може призвести, як мінімум, до витоку критично важливих даних та інформації всередині компанії.

У зв'язку з цим бажано було б реалізувати низку технічних заходів, спрямованих на оцінку захищеності комп'ютерних систем і мереж шляхом часткового моделювання поведінки зовнішніх зловмисників (тих, хто немає засобів доступу до системи) і внутрішніх зловмисників (тих, хто має певний рівень прав доступу).

Такий процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах. Аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей. Також корисно визначити процедури доступу та обміну інформацією в мережі та використання певних програмних засобів в середині компанії.

Варто звернути увагу також на можливість використання програмного забезпечення для захисту від витоку інформації, контролю продуктивності команди за ПК та управління подіями інформаційної безпеки. Однак, в даній ситуації при прийняті рішення щодо впровадження такого ПЗ необхідно підготувати певний бекграунд для того щоб діяти в межах закону відповідно до обраної юрисдикції.

4. Юридична безпека IT компанії

Дуже часто власники та керівники IT-компаній не приділяють достатньої та належної уваги юридичним аспектам свого бізнесу. Часто відносини з працівниками та підрядниками не регулюються або регулюються "абияк".

Маючи на руках підписаний договір про нерозголошення (NDA), адаптований під визначену діяльність для конкретного учасника правовідносин, який підписався під нерозголошенням комерційної таємниці, може змусити такого учасника декілька разів подумати перед тим, як комусь щось розповідати.

Доречною буде наявність підписаної угоди про не конкуренцію (NCA) в додаток до основного договору з контрагентом (особливо, якщо така діяльність здійснюється за межами України).

Ретельний аналіз укладених контрактів може запобігти можливим негативним наслідкам для IT-компанії в майбутньому, а також узгодити та

змінити окремі положення цих контрактів відповідно до вимог законодавства країн, в яких ІТ-компанія та її торгові партнери здійснюють свою діяльність.

5. Економічна (фінансова) безпека

Стан, в якому життєво важливі інтереси ІТ-бізнесу захищені від недобросовісної конкуренції, не компетентних рішень та недосконалого законодавства, а також його здатність протистояти цим загрозам і досягати цілей своєї діяльності, в цілому є економічною безпекою підприємства.

- Важливим аспектом в цьому ключі є:
- забезпечення високої фінансової ефективності роботи;
- підтримка фінансової стійкості та незалежності підприємства;
- досягнення високої конкурентноздатності;
- забезпечення високої ліквідності активів компанії;
- підтримка належного рівня ділової активності;
- забезпечення захисту інформаційного поля і комерційної таємниці;
- ефективна організація безпеки капіталу та майна підприємства, а також його комерційних інтересів.

Змістовний, якісний аналіз цих аспектів діяльності ІТ-компанії дозволяє швидко виявити слабкі місця у фінансовій безпеці, впровадити найбільш прийнятну економічну модель, скоригувати ключові аспекти обраної операційної моделі компанії тощо.

1.1.1.1 Захист конфіденційної інформації в ІТ-компаніях

Конфіденційність інформації вимагає, щоб особа, яка має доступ до певної інформації, не розголошувала цю інформацію третім особам без згоди її власника. Оскільки поняття "конфіденційність" в діяльності ІТ-компаній може бути багатогранним, питання захисту приватності також є багатогранним. В контексті діяльності компанії може бути важливим запобігти витоку унікальної клієнтської бази або злому серверів, або ж необхідно зберегти конфіденційну

інформацію про проекти, які знаходяться в стадії розробки, але можуть підірвати ринок, тощо. Тому розуміння способів і засобів захисту конфіденційної інформації компанії є одним із ключів до успішного управліннякомпанією.

Збереження внутрішньої інформації ІТ компанії в таємниці вигідно для кожного бізнесу через декілька досить очевидних причин:

- Конкурентна перевага: ще Ротшильди сказали: «Що той, хто володіє інформацією – володіє світом». Якщо у нас з'явилася ідея революційного проекту або неймовірного технологічного рішення, ми точно незахочемо, щоб про нього дізналися наші конкуренти. Зберігати в таємниці інформацію про проекти, корпоративну культуру, методики підбору персоналуі т.д. – означає завжди мати туза в рукаві.
- Цінність конфіденційної інформації: особливо у випадку з ІТ компаніями, вартість інформації або даних, якими вони володіють (клієнтська база, унікальний софт, алгоритми роботи і т.д.) може у багато разів перевищувати вартість їх матеріальних активів (офісне приміщення, обладнання, техніка і т.д.). У разі розголошення клієнтської бази або інформації про проект втрати компанії в моменти можуть бути колосальними, не кажучи про втрати в перспективі.
- Робота з іноземними клієнтами: в своїй більшості, клієнти вітчизняних ІТ компаній знаходяться за кордоном – США, Європа, Великобританія і т.д. З одного боку, зарубіжні контрагенти цінують, коли бізнес ведеться чітко, правильно, надійно і в повній відповідності з законом (що включає в себе налагоджені механізми захисту інформації). З іншого боку, при роботі з іноземними клієнтами ми отримуємо в розпорядження їх секрети, їх інформацію, а тому стаємо відповідальними вже не тільки перед самими собою, а й перед клієнтами. Тому для спокійного сну вночі потрібно мати надійну систему захисту.

- Вимоги законодавства: банальна, але через це не менш важлива причина. Законодавство кожної країни встановлює свої власні, але незмінно жорсткі та конкретні зобов’язання щодо захисту конфіденційної інформації і персональних даних. Якщо наша компанія не буде їх дотримуватися – ми легко можете потрапити до суду, де зустрітись як з представниками держорганів, так і з клієнтом / замовником, з конфіденційною інформацією якого трапилася неприємність.

По-перше, необхідно визначити, що є конфіденційною інформацією в компанії. У кожній компанії є як стандартні категорії такої інформації (наприклад, заробітна плата, умови праці, бізнес-процеси тощо), так і спеціальні категорії, які залежать від діяльності компанії (наприклад, паролі та системи доступу для тих, хто орендує приміщення).

Після визначення переліку конфіденційної інформації необхідно описати тип захисту.

Перший тип захисту-це документування. Це пов'язано з необхідністю зафіксувати всі принципи, рішення, правила, методи захисту тощо на папері. Це має включати наступні дії:

- Складання і підписання угоди про нерозголошення конфіденційної інформації (NDA) з кожним із співробітників, клієнтів, інвесторів, постачальників, підрядників, контрагентів і т.д. Для душевного спокою, NDA варто підписувати навіть зі стажерами і відвідувачами, так як вони теж можуть, випадково чи ні, отримати доступ до конфіденційної інформації.
- Складання Положення компанії про захист конфіденційності. Вимога до наявності такого документа найчастіше встановлюється законодавством для компаній, які працюють зі співробітниками за трудовими договорами. У той же час, для компаній, які працюють за схемою договорів з підрядниками, складання такого документа також може бути вигідним. З кожного співробітника має бути письмове зобов’язання, в якому співробітник

вказує, що ознайомився з текстом Положення і зобов'язується не порушувати його норми.

- Складання внутрішніх процедур поводження з конфіденційною інформацією. Ці документи будуть суто внутрішніми документами ІТ компанії. Вони повинні регламентувати порядок і правила доступу до конфіденційної інформації; її пересилання; доступу до неї третіх осіб; перелік співробітників, яким дозволено доступ до тієї чи іншої інформації; алгоритм дії в разі порушення захисту конфіденційної інформації і т.д. Для складання цих документів ІТ компанії слід звернутися до профільної юридичній фірмі, яка б проконсультувала компанію з цього питання, провела аналіз її рівня захисти конфіденційної інформації і склала необхідні документи.

Другий вид захисту – технічний. Він полягає в необхідності реалізувати на ділі всі наші рішення і плани. Це повинно включати в себе наступні дії:

- Визначити, хто має доступ до конфіденційної інформації на даний момент. Це дозволить зрозуміти, в якому масштабі потрібно впроваджувати захисні алгоритми, які місця в питанні захисту є найбільш уразливими і т.д. Одним з найпоширеніших підходів є рішення не давати повного доступу до конфіденційної інформації нікому, в тому числі – ІТ-фахівцям.

- Завжди важлива не тільки оцінка ризиків, але і подальший моніторинг. Тому після аналізу ситуації з доступом до конфіденційної інформації необхідно контролювати, хто і як користується, пересилає, змінює, доповнює, видаляє, переглядає і т.д. цю інформацію. Також, у разі будь-якого порушення системи захисту така інформація і аналітика буде на вагу золота.

- Внутрішня система для роботи і спілкування співробітників. Створення корпоративної чат-системи між співробітниками добре тим, що, по-перше, це дозволяє на 99% забезпечити оборот і передачу конфіденційної інформації тільки всередині таких корпоративних систем, а не через відкриті джерела (наприклад, Telegram, Facebook і т.д.), а по-друге, збирати дані про

будь-які операції з конфіденційною інформацією на випадок можливого порушення її захисту.

- Паролі. Переконайтеся, що доступ до всього знаходиться під захистом. Криптографічне шифрування ПК, паролі доступу до папок з конфіденційною інформацією, особисті паролі доступу в корпоративну систему для кожного співробітника і т.д. – все це є очевидно необхідним, а також дозволяє збирати дані про доступ до конфіденційної інформації, які можуть стати в нагоді для аналітики.
- Система захисту від кібератак. Така система базова і можевключати в себе превентивні засоби захисту, процедуру резервного копіювання конфіденційної інформації, прописаний алгоритм дії в разі кібератаки або іншого порушення захисту конфіденційної інформації і т.д.

IT-компаніям, які орендують великі офіси, може знадобитися вжити певних заходів. Для таких компаній доцільно мати обов'язкову багаторівневу систему доступу (вхід - відділ - кабінет), відео спостереження, службу безпеки та захищену мережу Wi-Fi.

Загалом, захист конфіденційної інформації-справа не п'ятихвилинна. Він завжди має бути спланованим і виваженим, і навіть найменший пролом може призвести до досить серйозних, якщо не незворотних, втрат.

Важливо також пам'ятати, що це має бути інклюзивний процес. Підписати угоду з усіма працівниками, не запровадивши реального механізму конфіденційності, або навпаки - розробити та впровадити хороші системи та алгоритми захисту інформації, працювати без документації "під чесне слово"- жоден з цих варіантів не спрацює.

1.1.1.2 Оцінка IT ризиків

Комп'ютерне обладнання та програмне забезпечення, що використовується в компанії, повинно постійно оновлюватися. Інформаційні

технології повинні відповідати потребам і цілям бізнесу, що вимагає управління та бухгалтерського обліку, а професійний аналіз ІТ може надати достовірну інформацію про стан інформаційно-технологічних ресурсів компанії. Всього цього можна досягти за допомогою ІТ-аудиту.

Аудит інформаційної безпеки полягає в розумінні, управлінні, контролі та зменшенні ризиків для критично важливих активів компанії. При роботі з даними в мережі необхідно оцінювати ризики інформаційної безпеки організації.

Аудит кібербезпеки – це можливість уникнути незапланованих ризиків, пов’язаних з відмовою або неправильним використанням ІТ. На Рисунку 1.1 наведено ризики кібербезпеки.

Рисунок 1.1 Ризики кібербезпеки

Кібербезпека - це комплексне питання, що включає багато факторів і стандартів, і це одна з причин, чому багато організацій ставлять кібербезпеку на другий план. На жаль, безпека не може бути гарантована на 100%, тому важливо застосовувати підхід, заснований на оцінці ризиків, який фокусується на пріоритетах і ризиках.

Аудит інформаційної безпеки містить докладний опис конкретного фінансового збитку, який ІТ-ризики можуть нанести організації. Наприклад,

судові витрати, простої в роботі й пов'язані з цим втрати прибутку, а також втрачений бізнес через недовіру клієнтів. Найважливіші питання щодо IT-ризиків представлені Рисунку 1.2.

Рисунок 1.2 – Найважливіші питання щодо IT-ризиків

Залишається лише визначити, що спричиняє ризики і кого потрібно від них захистити.

Після визначення цілей управління ІБ необхідно проаналізувати проблеми, які перешкоджають наближенню до цільового стану. На цьому рівні процес аналізу ризиків спускається до традиційних понять ІБ, таких як інформаційна інфраструктура та зловмисники, загрози та вразливості. Для оцінки ризиків недостатньо ввести стандартну модель вторгнення, яка ізолює всі вторгнення за доступом до активу або знанням структури активу.

Такий поділ допомагає визначити, які загрози можуть бути спрямовані на актив, але не дає відповіді на питання, чи можуть бути ці загрози в принципі реалізовані. У процесі аналізу ризиків необхідно оцінити вмотивованість порушників під час реалізації загроз. При цьому під порушником мається на

увазі не абстрактний зовнішній хакер або інсайдер, а сторона, яка зацікавлена в отриманні вигоди шляхом порушення безпеки активу.

Як і у випадку з вибором початкових заходів з ІС, початковуінформацію щодо моделювання зловмисника слід отримати від вищого керівництва, яке розуміє позицію організації на ринку, конкурентів та очікувані типи методів атак. Інформація, необхідна для розробки моделі зловмисника, може бути отримана з професійних досліджень порушень комп'ютерної безпеки в аналізованій сфері бізнесу. Добре розроблена модель зловмисника повинна доповнювати цілі безпеки організації, визначені під час оцінки активів.

Моделювання загроз та виявлення вразливостей нерозривно пов'язані зі створенням інвентаризації середовища інформаційних активів організації. Сама пособі інформація не зберігається і не обробляється. Доступ до інформації забезпечується через інформаційну інфраструктуру, яка автоматизує бізнес-процеси організації. Важливо розуміти, як пов'язані міжсобою інформаційна інфраструктура та інформаційні активи організації.

З точки зору управління ІС, важливість інформаційної інфраструктури можна визначити лише після того, як буде з'ясовано взаємозв'язок між інформаційними активами та інфраструктурою. Якщо процес підтримки та експлуатації інформаційної інфраструктури в організації регламентований і прозорий, збір інформації, необхідної для виявлення загроз та оцінки вразливостей, значно спрощується.

Розробка моделей загроз - це завдання для фахівців з безпеки, які добре розуміють, як зловмисники можуть отримати несанкціонований доступ до інформації, порушуючи периметр безпеки або використовуючи методи соціальної інженерії. При розробці моделі загроз сценарій можна описати як низку послідовних кроків для реалізації загрози. Використання вразливостей системи рідко реалізує загрозу за один крок.

Модель загроз повинна включати всі загрози, виявлені в результаті відповідних процесів управління ІС, таких як управління вразливостями та управління інцидентами. Слід пам'ятати, що загрози повинні бути проранжовані відповідно до рівня ймовірності їх реалізації. Тому в процесі розробки моделі загроз слід визначити найбільш важливі фактори, щовпливають на її реалізацію.

1.2 Політика безпеки українських ІТ-компаній

Політика безпеки ґрунтується на аналіз і ризиків, визначених як реалістичні для інформаційних систем організації. Після аналізу ризиків і визначення стратегії захисту розробляється програма інформаційної безпеки. На цю програму виділяються ресурси, призначаються відповідальні особи та визначаються процедури контролю за виконанням програми.

У широкому сенсі політика безпеки визначається як система задокументованих управлінських рішень, спрямованих на забезпечення безпеки організації. У більш вузькому сенсі під політикою безпеки зазвичай розуміють локальний нормативний документ, який визначає вимоги до безпеки, системи або процедури протидії, а також обов'язки і механізми контролю співробітників організації щодо конкретних сфер безпеки. Перш ніж приступити до розробки власне політики інформаційної безпеки, необхідно розібратися з основними поняттями, що використовуються.

1.2.1 Політика інформаційної безпеки ІТ-компанії

Інформація - це відомості (повідомлення, дані), незалежно від форми їх вираження.

Інформаційна безпека (ІБ) - це стан захищеності, за якого забезпечується формування, використання та розвиток інформаційного середовища суспільства в інтересах громадян, організацій і держави.

Поняття "інформація" сьогодні використовується досить широко та різнобічно.

Забезпечення інформаційної безпеки – це не разовий захід. Це безперервний процес створення та впровадження найбільш раціональних методів, прийомів і способів удосконалення та розвитку системи безпеки, постійного моніторингу її стану та виявлення слабких місць і протиправної діяльності.

Інформаційна безпека може бути забезпечена лише шляхом комплексного використання всіх доступних засобів захисту в усіх структурних елементах виробничої системи та на всіх етапах циклу обробки інформації. Максимальна ефективність досягається тоді, коли всі використовувані інструменти, методи і заходи об'єднані в один комплексний механізм - систему інформаційної безпеки. При цьому функціонування системи потребує моніторингу, оновлення та доповнення у відповідь на зміну зовнішніх та внутрішніх умов. Також варто враховувати, що умови можуть змінюватися непередбачено.

Можна назвати такі види вимог до безпеки:

- функціональні: відповідають активному аспекту захисту, що пред'являються до функцій безпеки та механізмів, які їх реалізують;
- вимоги довіри: відповідають пасивному аспекту, що висуваються до технології, процесу розробки та експлуатації.

Дуже важливо, що безпека розглядається не статично, а у прив'язці до життєвого циклу об'єкта оцінки. Виділяються такі етапи:

- визначення призначення, умов застосування, цілей та вимог безпеки;
- проектування та розробка;

- випробування, оцінка та сертифікація;
- використання та експлуатація.

Отже, докладніше зупинимося на функціональних вимогах безпеки. Вони включають:

- захист даних користувача;
- захист функцій безпеки (вимоги відносяться до цілісності і контролю даних сервісів безпеки та реалізують їх механізми);
- управління безпекою (вимоги цього класу відносяться доуправління атрибутами та параметрами безпеки);
- аудит безпеки (виявлення, реєстрація, зберігання, аналіз даних, що стосуються безпеки об'єкта оцінки, реагування на можливе порушення безпеки);
- приватність (захист користувача від розкриття та несанкціонованого використання його ідентифікаційних даних);
- використання ресурсів (вимоги до доступності інформації);
- зв'язок (аутентифікація сторін);
- довірений маршрут/канал (для зв'язку із сервісами безпеки).

Відповідно до цих вимог потрібно формувати систему інформаційної безпеки організації.

Система інформаційної безпеки організації включає напрямки:

- нормативні;
- організаційні (адміністративні);
- технічні;
- програмні.

Для того, щоб повністю розуміти ситуацію підприємства во всіх сферах безпеки, необхідно розробити концепцію інформаційної безпеки. Це встановлює системний підхід до питання захисту інформаційних ресурсів і забезпечує систематизований набір цілей, завдань, принципів побудови та комплекс заходів для забезпечення інформаційної безпеки на підприємствах.

В основі системи інформаційного контролю IT-компанії повинні лежати наступні принципи (рис.1.3):

- забезпечення захисту існуючої інформаційної інфраструктури підприємства від втручання зловмисників;
- забезпечення умов для локалізації та мінімізації можливої шкоди;
- виключення появи на стадії причин виникнення джерел загроз;
- забезпечення захисту інформації за трьома основними видами загроз (доступність, цілісність, конфіденційність).

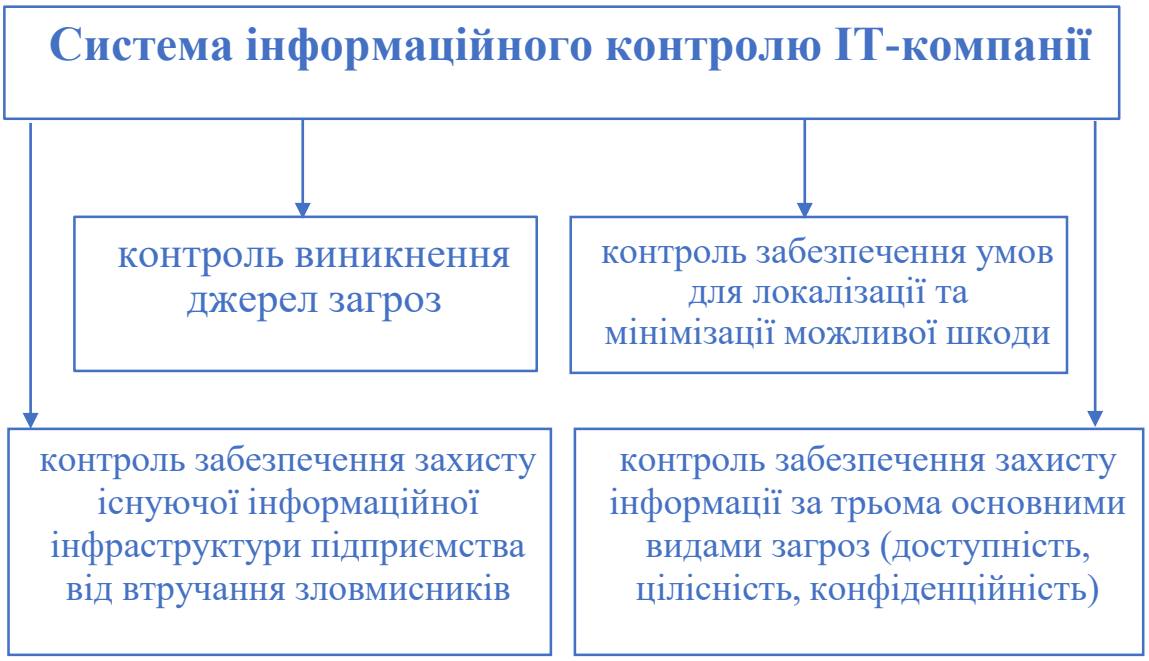


Рисунок 1.3 Система інформаційного контролю IT-компанії

Розв'язання вищезгаданих завдань досягається шляхом:

- регламентація дій користувачів роботи з інформаційною системою;
- регламентація дій користувачів роботи з базою даних;
- єдині вимоги до надійності технічних засобів та програмного забезпечення;
- процедури контролю роботи інформаційної системи (протоколювання подій, аналіз протоколів, аналіз мережевого трафіку, аналіз роботи технічних засобів);

Політика інформаційної безпеки включає основний документ – «Політика безпеки». У ньому в цілому описана політика безпеки організації, загальні становища, а як і з усіма аспектами політики зазначені відповідні документи:

- інструкція щодо регламентації роботи користувачів;
- посадова інструкція адміністратора локальної мережі;
- посадова інструкція адміністратора бази даних;
- інструкція щодо роботи з ресурсами Інтернет;
- інструкція щодо організації парольного захисту;
- інструкція з організації антивірусного захисту.

Документ "Політика безпеки" містить основні положення. На основі нього будується програма забезпечення інформаційної безпеки, будуються посадові інструкції та рекомендації.

• Інструкція з регламентації роботи користувачів локальної мережі організації регулює порядок допуску користувачів до роботи у локальній мережі обчислювальної мережі організації, а також правила поводження з інформацією, що захищається, оброблюється, зберігається і передається в організації.

• Посадова інструкція адміністратора локальної мережі визначає обов'язки адміністратора локальної мережі, що стосуються забезпечення інформаційної безпеки.

• Посадова інструкція адміністратора бази даних визначає основні обов'язки, функції та права адміністратора бази даних. У ній дуже докладно описані всі посадові обов'язки та функції адміністратора бази даних, а також права та відповідальність.

• Інструкція по роботі з ресурсами Інтернет відображає основніправила безпечної роботи з мережею інтернет, також містить перелік допустимих недопустимих дій під час роботи з ресурсами інтернет.

• Інструкція з організації антивірусного захисту визначає основні положення, вимоги до антивірусного захисту інформаційної системиорганізації, всі аспекти пов'язані з роботою антивірусного програмного забезпечення, а також відповідальність у разі порушення антивірусного захисту.

• Інструкція з організації парольного захисту регламентує організаційно-технічне забезпечення процесів генерації, зміни та припинення дії паролів (видалення облікових записів користувачів). А також регламентованідії користувачів та обслуговуючого персоналу під час роботи з системою.

Таким чином, основою для організації процесу захисту є політика безпеки, яка існує для того, щоб визначити, як і від яких загроз має бути захищена інформація в інформаційній системі.

Політика безпеки – це комплекс правових, організаційних і технічних заходів інформаційної безпеки, прийнятих конкретною організацією. Іншими словами, політика безпеки містить набір умов, за яких користувачі можуть отримати доступ до ресурсів системи без шкоди для якості інформаційної безпеки системи. Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що різні заходи безпеки (апаратні, програмні, фізичні, організаційні тощо) повинні застосовуватися одночасно під централізованим контролем.

Політика інформаційної безпеки-це набір документів, які регламентують роботу співробітників і описують основні правила поводження з інформацією, інформаційними системами, базами даних, локальними мережами та інтернет-ресурсами. Важливо розуміти місце політики інформаційної безпеки в загальній системі управління організацією.

Нижче наведено загальні організаційні заходи, пов'язані з політикою безпеки. На процедурному рівні можна виділити такі класи заходів:

- управління персоналом;
- фізичний захист;

- підтримання працездатності
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

Управління персоналом починається з прийому працівників, проте ще до цього слід визначити комп'ютерні привілеї, пов'язані з посадою. Існує два загальних принципу, які слід мати на увазі:

- розподіл обов'язків;
- мінімізація привілеїв.

Принцип розподілу обов'язків описує, як розподіляються ролі та обов'язки таким чином, щоб жодна особа не порушувала ключові організаційні процеси. Наприклад, небажано, щоб одна особа здійснювала великі платежі від імені організації. Надійніше доручити обробку заявок на такі платежі одному співробітнику, а перевірку автентичності заявки - іншому. Іншим прикладом є процедурні обмеження на роботу супер користувачів. Пароль супер користувача може бути штучно розділений, при цьому перша частина передається одному співробітнику, а друга - іншому. У такому випадку лише двоє людей можуть виконувати важливі дії з управління інформаційною системою, що зменшує ймовірність помилок і несанкціонованоговикористання.

Принцип найменших привілеїв вимагає, щоб користувачам надавалися права доступу, необхідні їм для виконання своїх обов'язків. Мета цього принципу зрозуміла: щоб зменшити шкоду, спричинену випадковими або навмисними неправомірними діями. Попередні посадові інструкції дозволяють оцінити важливість посади та спланувати процедури перевірки та відбору кандидатів. Чим відповідальніша посада, тим ретельніше потрібно перевіряти кандидата, зокрема наводити довідки про нього, а в деяких випадках - розмовляти з колишніми колегами. Ці процедури займають багато часу і коштують дорого, і не варто їх ускладнювати. Однак було б нерозумно повністю відмовитися від попередніх перевірок, щоб уникнути випадкового

прийняття на роботу людини з кримінальним минулим або психічним захворюванням.

Після того, як кандидат визначений, він повинен пройти навчання. Як мінімум, слід пояснити посадові обов'язки, а також політику та процедури інформаційної безпеки. Бажано, щоб кандидати розуміли існуючі заходи безпеки до того, як вони займуть посаду, і до того, як їм буде надано системний обліковий запис з ім'ям користувача, паролем і повноваженнями.

1.2.2 Методи забезпечення інформаційної безпеки

Сьогодні існує безліч способів забезпечити інформаційну безпеку:

- засоби ідентифікації та автентифікації користувачів;
- засоби шифрування інформації, що зберігається на комп'ютерах та передається по мережах;
- міжмережеві екрани;
- віртуальні приватні мережі;
- засоби контентної фільтрації;
- інструменти перевірки цілісності вмісту дисків;
- засоби антивірусного захисту;
- системи виявлення вразливостей мереж та аналізатори мережевих атак.

Системи автентифікації (або ідентифікації), авторизації та контролю. Ідентифікація та авторизація є ключовими елементами інформаційної безпеки. Функція автентифікації відповідає за визначення того, до яких ресурсів може отримати доступ конкретний користувач. Функція управління полягає у наданні користувачеві певної ідентифікаційної функції в мережі та визначенні діапазону дій, дозволених цьому користувачеві.

Системи шифрування можуть мінімізувати несанкціонований доступ до даних, що зберігаються на жорстких дисках та інших носіях, а також втрати,

якщо інформацію перехоплять під час передачі електронною поштою або за допомогою мережевого протоколу. Метою цього заходу безпеки є забезпечення конфіденційності. Основними вимогами до систем шифрування є високий рівень криптографічної безпеки та легальність використання в Україні або інших країнах.

Брандмауер – це система або комбінація систем, яка утворює захисний бар'єр між двома або більше мережами і захищає пакети даних від несанкціонованого входу і виходу з мережі. Основний принцип роботи брандмауера полягає в перевірці відповідності кожного пакету даних IP-адресі, за якою він входить в мережу або виходить з неї, на основі дозволених адрес. Таким чином, брандмауери значно розширюють можливості сегментації інформаційних мереж і контролю за розподілом даних.

Говорячи про криптографію і брандмауери, для вирішення питань конфіденційності та цілісності даних при передачі даних по відкритих каналах зв'язку можна використовувати захищену віртуальну приватну мережу (VPN). Використання VPN зводиться до вирішення трьох основних завдань:

• захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу);

• захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, що здійснюється через інтернет;

• захист інформаційних потоків між окремими програмами всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється із внутрішніх мереж).

Фільтрація вмісту вхідної та вихідної електронної пошти є ефективним засобом запобігання втрат і конфіденційної інформації. Перевірка електронних повідомлень і вкладень відповідно до правил, встановлених організацією, також може захистити компанію від відповідальності в судовому процесі та захистити від спаму. Інструменти фільтрації вмісту можуть перевіряти всі

поширені формати файлів, такі як стиснуті файли та графічні файли. При цьому пропускна здатність мережі залишається практично незмінною.

Технологія перевірки цілісності дозволяє мережевим адміністраторам або іншим авторизованим користувачам відстежувати всі зміни на робочих станціях і серверах. Це дозволяє виявити будь-які операції з файлами (модифікація, видалення або просто відкриття), а також ідентифікувати вірусну активність, несанкціонований доступ авторизованих користувачів або крадіжку даних. Цей контроль забезпечує основу для аналізу контрольної суми (CRC) файлу.

Сучасні антивірусні технології дозволяють виявити майже всі відомі віруси. Антивірусні технології можуть виявляти більшість відомих вірусів, порівнюючи код підозрілих файлів зі зразками, що зберігаються в антивірусних базах даних. Крім того, розроблено методи моделювання поведінки для виявлення новостворених вірусів. Виявлені об'єкти можна обробити, помістити в карантин або видалити. Антивірус може бути встановлений на робочих станціях, файлових серверах, поштових серверах і брандмауерах та працює практично з усіма популярними операційними системами (Windows, Unix, Linux системи, Novell) на різних типах процесорів.

Спам-фільтри значно зменшують непродуктивні трудовитрати, пов'язані з аналізом спаму, знижують трафік і навантаження на сервер, покращують психологічний клімат у колективі та зменшують ризик залучення співробітників до шахрайських транзакцій. Крім того, спам-фільтри знижують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ті, яких ще немає в антивірусних базах), часто мають спам-підписі відфільтровуються. Однак позитивні ефекти спам-фільтрів можуть бути нівельовані, якщо вони видаляють корисні ділові чи особисті повідомлення абопозначають їх як спам разом із небажаною поштою.

Величезні збитки, яких зазнають компанії через вірусні та хакерські атаки, значною мірою зумовлені вразливістю програмного забезпечення. Ці

вразливості можна виявити до початку атаки за допомогою систем виявлення мережевих вразливостей та аналізаторів атак. Ці програмні інструменти безпечно імітують поширені методи атак і визначають, що хакери бачать у мережі та як вони використовують її ресурси.

Щоб протистояти природним загрозам інформаційній безпеці, компаніям необхідно розробити та впровадити комплекс процедур для запобігання надзвичайним ситуаціям (наприклад, фізичний захист даних від пожежі) та мінімізації збитків, якщо такі ситуації трапляються. Одним з основних способів запобігти втраті даних є резервне копіювання, яке суворо дотримується встановлених процедур (наприклад, частота, тип носія, спосіб зберігання копій).

Безпека інформаційної системи залежить від середовища, в якому вона працює. Необхідно вжити заходів для захисту будівлі та прилеглої території, допоміжної інфраструктури, комп'ютерного обладнання та носіїв даних.

Розглянемо такі напрямки фізичного захисту:

- фізичне управління доступом;
- захист підтримуючої інфраструктури;
- захист мобільних систем.

Заходи фізичного контролю доступу дозволяють контролювати та обмежувати доступ співробітників і відвідувачів за необхідності. Можна контролювати як усю будівлю організації, так і окремі приміщення, наприклад, сервери та комунікаційне обладнання.

Допоміжна інфраструктура включає системи електропостачання, водопостачання та теплопостачання, кондиціонування повітря та телекомунікації. В принципі, вимоги до цілісності та доступності накладаються так само, як і до інформаційних систем. Для забезпечення цілісності обладнання повинно бути захищене від крадіжок і пошкоджень. Для підтримкидоступності необхідно вибирати обладнання з максимальним інтервалом між

відмовами, резервувати критичні компоненти і завжди мати в наявності запасні частини.

Загалом, при виборі засобів фізичного захисту слід проводити аналіз ризиків. Наприклад, при прийнятті рішення про придбання джерела безперебійного живлення слід враховувати якість електропостачання в будівлі, характер і тривалість перебоїв, вартість наявного джерела живлення та можливі втрати через аварії (наприклад, вихід з ладу обладнання, призупинення роботи організації).

Розглянемо низку заходів, вкладених у підтримку працездатності інформаційних систем. Саме в цій галузі таїться найбільша небезпека. До втрати працездатності, а саме пошкодження апаратури, руйнування програм та даних можуть призвести ненавмисні помилки системних адміністраторів та користувачів.

Основна проблема багатьох організацій – недооцінка факторів безпеки у повсякденній роботі. Дорогі засоби безпеки втрачають сенс, якщо вони погано документовані, конфліктують з іншим програмним забезпеченням, а пароль системного адміністратора не змінювався з моменту встановлення.

Для повсякденної діяльності, спрямовані на підтримку працездатності інформаційної системи можна назвати такі дії:

- підтримка користувачів;
- підтримка програмного забезпечення;
- конфігураційне управління;
- резервне копіювання;
- керування носіями;
- документування;
- регламентні роботи.

Підтримка користувачів-це насамперед надання консультацій та допомоги у вирішенні різних проблем. Дуже важливо вміти виявляти проблеми з інформаційною безпекою в процесі опитування. Труднощі в роботі

користувача з комп'ютером можуть бути пов'язані з вірусною інфекцією. Бажано записати запитання користувача, виявити типові помилки та видати пам'ятку з рекомендаціями для поширених ситуацій.

Підтримка програмного забезпечення є одним з найважливіших засобів забезпечення цілісності інформації. Перш за все, необхідно стежити за тим, яке програмне забезпечення встановлено на комп'ютері. Якщо користувачі встановлюють програми з власної ініціативи, це може призвести до зараження вірусами та появи утиліт, які обходять засоби захисту. Також не виключено, що "самодіяльність" користувача може поступово вивести комп'ютер з ладу, і системному адміністратору доведеться виправляти ситуацію.

Другим аспектом підтримки програмного забезпечення є забезпечення відсутності несанкціонованих змін у програмі та контроль прав доступу до програми. Сюди входить підтримка еталонної копії програмної системи. Контроль зазвичай досягається за допомогою поєднання фізичного та логічного контролю доступу, а також використання утиліт перевірки та цілісності.

Керування конфігурацією дозволяє контролювати та реєструвати зміни, внесені до конфігурації програмного забезпечення. Перш за все, це повинно забезпечити страхування від випадкових або ненавмисних зміні, принаймні, дозволити повернутися до попередньої робочої версії. Фіксація змін полегшує відновлення поточної версії після збою.

Найкращий спосіб зменшити кількість помилок у рутинній роботі-це максимально автоматизувати її. Автоматизація та безпека взаємозалежні. Це пов'язано з тим, що люди, які найбільше зацікавлені у спрощенні своєї роботи, насправді мають найкращі системи інформаційної безпеки.

Резервне копіювання необхідно для відновлення програм та даних після аварій. І тут доцільно автоматизувати роботу, як мінімум, сформувавши комп'ютерний розклад створення повних та інкрементальних копій, а як максимум – скориставшись відповідними програмними продуктами. Потрібно також налагодити розміщення копій у безпечному місці, захищеному від

несанкціонованого доступу, пожеж, протікання, тобто всього, що може призвести до крадіжки або пошкодження носіїв. Доцільно мати кілька екземплярів резервних копій частину з них зберігати поза територією організації, захищаючись таким чином від великих аварій та аналогічних інцидентів. Іноді в тестових цілях слід перевіряти можливість відновлення інформації з копій.

Керувати носіями необхідно для забезпечення фізичного захисту та обліку дискет, стрічок, друкованих видач тощо. Керування носіями має забезпечувати конфіденційність, цілісність та доступність інформації, що зберігається поза комп'ютерними системами. Під фізичним захистом тут розуміється як відображення спроб несанкціонованого доступу, а й захист від шкідливих впливів довкілля (спеки, холоду, вологи, магнетизму). Управління носіями має охоплювати весь життєвий цикл – від закупівлі до виведення з експлуатації.

Документування – невід'ємна частина інформаційної безпеки. У вигляді документів оформляється майже все - від безпекової політики до журналуобліку носіїв. Важливо, щоб документація була актуальною, відображала саме поточний стан справ, причому у несуперечливому вигляді.

До зберігання одних документів (що містять, наприклад, аналіз уразливих місць системи та загроз) застосовні вимоги забезпечення конфіденційності, до інших, таких як план відновлення після аварій – вимоги цілісності та доступності (у критичній ситуації план необхідно знайти та прочитати).

Регламентні роботи – дуже серйозна загроза безпеці. Співробітник, який здійснює регламентні роботи, отримує винятковий доступ до системи, і це практично дуже важко проконтролювати, які саме дії він робить. Тут на перший план виходить ступінь довіри до тих, хто виконує роботу.

Політика безпеки, прийнята в організації, має передбачати набір оперативних заходів, спрямованих на виявлення та нейтралізацію порушень

режиму інформаційної безпеки. Важливо, щоб у подібних випадках послідовність дій була спланована заздалегідь, оскільки заходи слід вживати термінових та скоординованих. Реакція на порушення режиму безпеки має такі головні цілі:

- локалізація інциденту та зменшення шкоди, що завдається;
- запобігання повторних порушень.

Нерідко вимога локалізації інциденту і зменшення шкоди, що завдається, вступає в конфлікт з бажанням виявити порушника. У безпековій політиці організації пріоритети мають бути розставлені заздалегідь. Оскільки, як показує практика, виявити зловмисника дуже складно, насамперед слід дбати про зменшення шкоди. Жодна організація не застрахована від серйозних аварій, спричинених природними причинами, діями зловмисника, недбалістю чи некомпетентністю. У той самий час, кожна організація має функції, які керівництво вважає критично важливими, вони мають виконуватися попри що. Планування відновлювальних робіт дозволяє підготуватися до аварій, зменшити збитки від них та зберегти здатність до функціонування хоча б у мінімальному обсязі. Зазначимо, що заходи інформаційної безпеки можна розділити на три групи, залежно від того спрямовані вони на попередження, виявлення чи ліквідацію наслідків атак. Більшість заходів має запобіжний характер.

Процес планування відновлювальних робіт можна поділити на такі етапи:

- виявлення критично важливих функцій організації; встановлення пріоритетів;
- ідентифікація ресурсів, необхідні виконання критично важливих функцій;
- визначення переліку можливих аварій;
- розробка стратегії відновлювальних робіт;
- підготовка до реалізації обраної стратегії;

• перевірка стратегії.

Плануючи відновлювальні роботи, слід усвідомлювати, що повністю зберегти функціонування організації не завжди можливо. Необхідно виявити критично важливі функції, без яких організація втрачає своє обличчя, і навіть серед критичних функцій розставити пріоритети, щоб як найшвидше мінімальними витратами відновити роботу після аварії.

Ідентифікуючи ресурси, необхідних для виконання критично важливих функцій, слід пам'ятати, частина з них має некомп'ютерний характер. На цьому етапі бажано підключати до роботи спеціалістів різного профілю. Таким чином, існує велика кількість різних методів забезпечення інформаційної безпеки. Найбільш ефективним є застосування всіх даних методів у єдиному комплексі.

Сьогодні сучасний ринок перенасичений продуктами інформаційної безпеки. Багато компаній постійно вивчають існуючу пропозицію на ринку безпеки і розуміють, що їх ні попередні інвестиції в системи інформаційної безпеки є недостатніми, наприклад, через застарілість обладнання та програмного забезпечення. Тому вони шукають шляхи вирішення цієї проблеми. Є два варіанти: з одного боку, повна заміна системи інформаційної безпеки компанії, що вимагає значних інвестицій; з іншого боку, модернізація існуючої системи безпеки.

1.2.3 Комплексна IT-безпека компанії - на прикладі інструментів Microsoft

1.2.3.1 Кібератаки в Україні 2023: огляд загальної ситуації

Перш ніж перейти до огляду інструментів, які допоможуть виявити наявні вразливості та посилити кібербезпеку бізнесу, пропоную подивитися на загальну тенденцію хакерських атак за минулі півроку.

Перший масштабний інцидент стався в ніч з 13 на 14 січня, коли від дій кіберзлочинців постраждало близько 70 сайтів урядових організацій та банків. Продовж останніх 6 місяців ми регулярно бачимо заяви Урядової команди реагування на комп'ютерні надзвичайні події України про активність хакерів. За даними CERT-UA у першому півріччі 2022 року було зафіксовано 1350 кібератак.

Кіберзлочинці атакують не лише урядові сайти, а й представників фінансового, комерційного та телекомунікаційного секторів. На жаль, від протиправної діяльності страждають не лише ІТ-спеціалісти, які змушені оперативна ліквідовувати наслідки, але й ті, хто не бере участі у війні в цифровому середовищі: 5липня хакери перервали пряму трансляцію футбольного матчу між Україною та Уельсом на телеканалі All.tv. і замість відео запису матчу на екрані з'явилися російські пропагандистські кадри.

Безумовно, українські хакери теж атакують ворога. За даним Мінцифри з 26 лютого по 30 липня наша ІТ-армія заблокувала понад 600 російських онлайн-ресурсів.

1.2.3.2 Identities: рішення для управління ідентифікацією та доступом

В організації стратегії безпеки компанії будь-якого масштабу з будь-якої галузі, Microsoft рекомендує орієнтуватися на модель захисту Zero Trust. Вона адаптована до складного сучасного середовища й дозволяє захищати користувачів, пристрої, програми, дані та інфраструктуру. Це особливо актуально останні 2 роки, коли співробітники багатьох компаній почали працювати віддалено та з різних країн.

Модель нульової довіри працює за принципом, що чим більше сервісів ви налаштуєте для захисту інфраструктури вашої компанії, тим швидше ви зможете отримувати та реагувати на сповіщення про загрози безпеці.

Основою захисту з нульовою довірою і першим кроком у впровадженні політики безпеки є налаштування служби верифікації особи.

Деякі компанії продовжують використовувати базову автентифікацію, коли працівники використовують ім'я користувача та пароль при запиті доступу. Цей метод автентифікації більше не захищає конфіденційність облікових даних і залишає їх відкритими для зловмисників.

Тому базовим рівнем захисту Identity є сучасне налаштування автентифікації з використанням MFA, сучасного методу автентифікації (рис.1.4). Це додає ще один рівень захисту до процесу входу в систему.

Рисунок 1.4 Принцип дії MFA

Таким чином, MFA забезпечує додатковий рівень захисту при вході в обліковий записі, за даними Microsoft, може знизити ризик злому на 99,9%.

Також у ланці захисту Identities є ще одна вкрай важлива функція для управління доступом — Conditional-access (рис.1.5).

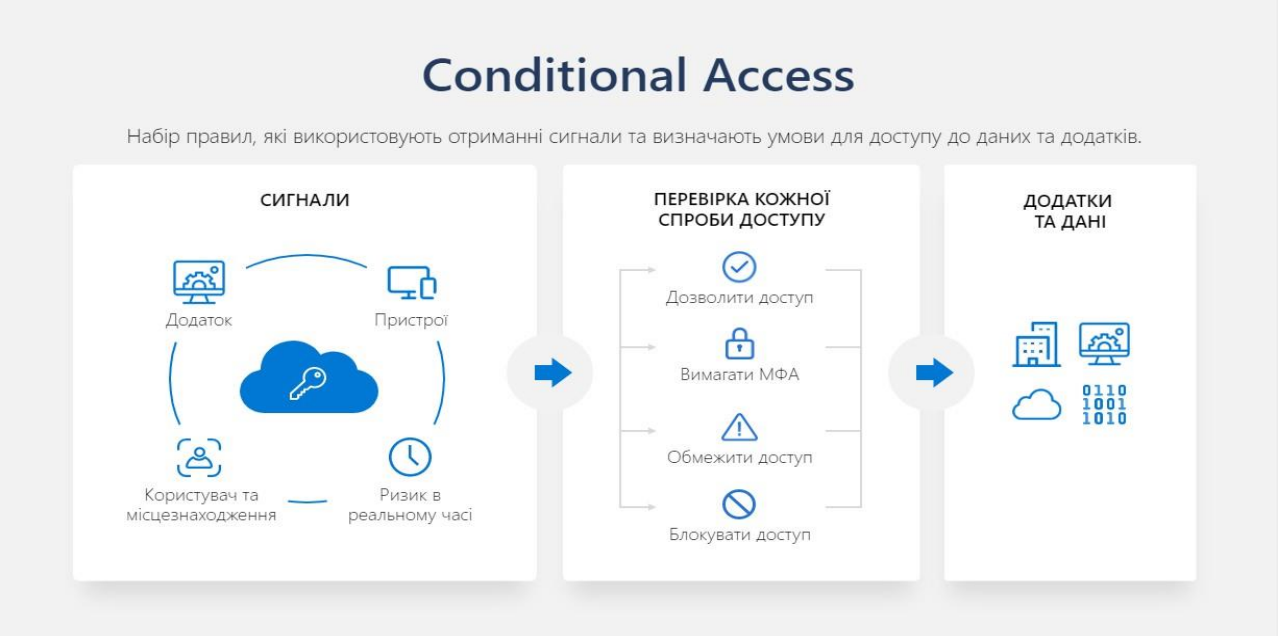


Рисунок 1.5 Набір правил управління доступом Conditional-access

Це налаштовує механізм перевірки кожного процесу підключення до корпоративної системи на основі створеного сценарію, з варіантами заборони доступу, дозволу без умов та умовного дозволу.

1.2.3.3 Endpoint: захист кінцевих точок компанії

У сучасних компаніях є великий «зоопарк» девайсів, які:

- управляються компанією,
- управляються співробітниками — BYOD,
- управляються сторонніми організаціями.

Це відкриває безмежні можливості для атак: за допомогою налаштування служб управління кінцевими точками, включаючи Microsoft Intune, можна здійснювати управління мобільними пристроями Intune (MDM) і управління програмним забезпеченням Intune (MAM) (рис.1.6).

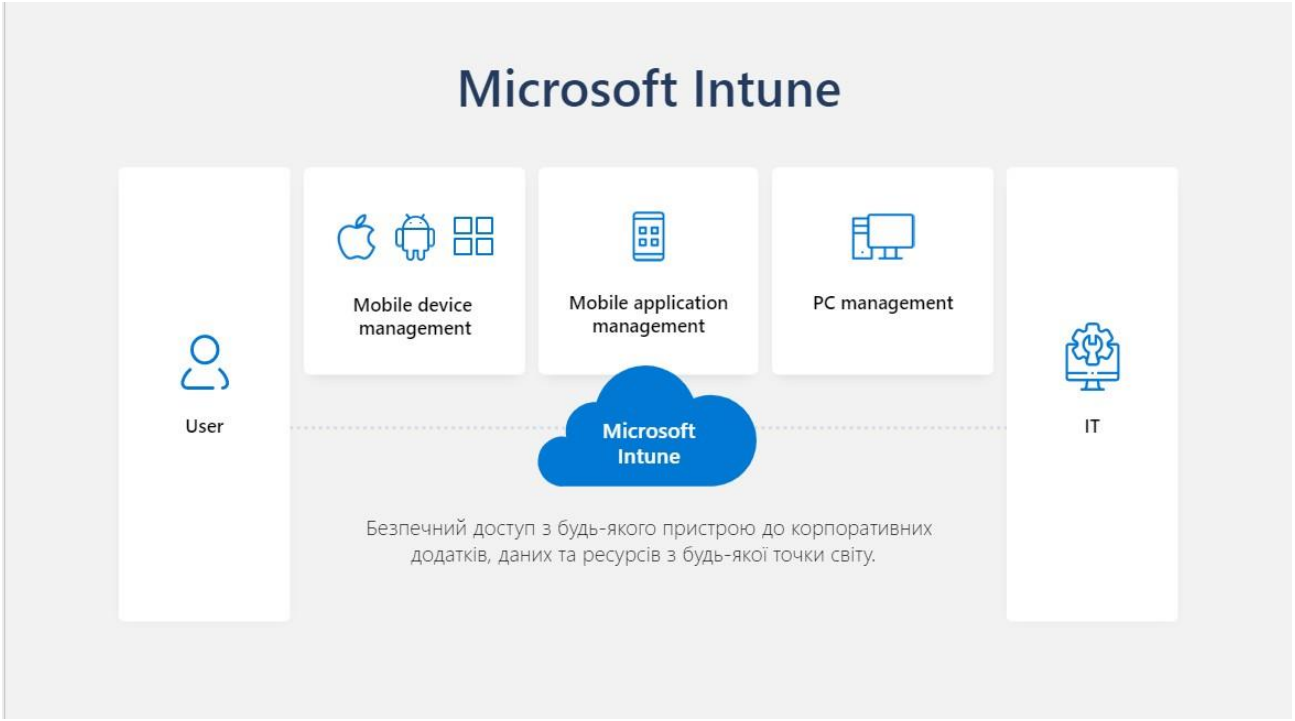


Рисунок 1.6 Intune (MAM)

Наприклад, якщо ви авторизувалися в обліковому записі компанії і маєте доступ до документів, що містять конфіденційну інформацію, вам потрібно переконатися, що цей документ не зберігається в незахищеному місці і що ним не можна ділитися в месенджерах, непов'язаних з компанією.

Рисунок 1.7 Політика захисту Intune (MAM)

За наявності політик захисту Intune MAM (рис.1.7), співробітники можуть передавати або копіювати дані тільки в довірених офісних програмах, таких як Word, Excel, Adobe Acrobat Reader, і зберігати їх тільки в надійних місцях, таких як OneDrive або SharePoint.

Intune MDM (рис.1.8) забезпечує централізоване керування кінцевими пристроями на платформах Android, iOS, Windows, MacOS.

Рисунок 1.8 Intune MDM

Наприклад, якщо пристрій загублено або викрадено, всі дані з нього можна видалити віддалено. Адміністратор обирає потрібний пристрій на панелі керування пристроєм і запускає процес видалення. Якщо опція "Зберегти дані" не вибрана, всі дані облікового запису будуть видалені. Цей процес повторюється до тих пір, поки результат не буде успішним, навіть після перезавантаження або вимкнення пристрою. Крім того, ця функція працює на Windows, Android, iOSiMacOS.

До речі, можливо також обмежувати встановлення додатків. Можна створити списки дозволених додатків в розділі Policy. Для цього необхідно лише додати посилання на додаток в магазині.

Для комплексного захисту кінцевих точок використовуємо сучасну платформу безпеки — Microsoft Defender for Endpoint.

Рішення дозволяє швидко зупиняти атаки, масштабувати ресурсибезпеки та покращувати захист для Windows, macOS, Linux, Android, iOS та мережевих пристроїв Microsoft Defender для кінцевих точок інструменти та аналітика дають змогу контролювати інфраструктуру, протидіяти сучасним загрозам і реагувати на оповіщення з єдиної інтегрованої платформи.

1.2.3.4 Data Protection: безпечна робота з корпоративними даними

У будь-якій компанії присутні об’єми даних, які необхідно захищати. Для цього у Microsoft є відповідні сервіси, які об’єднані у напрямок Data Protection (рис1.9).

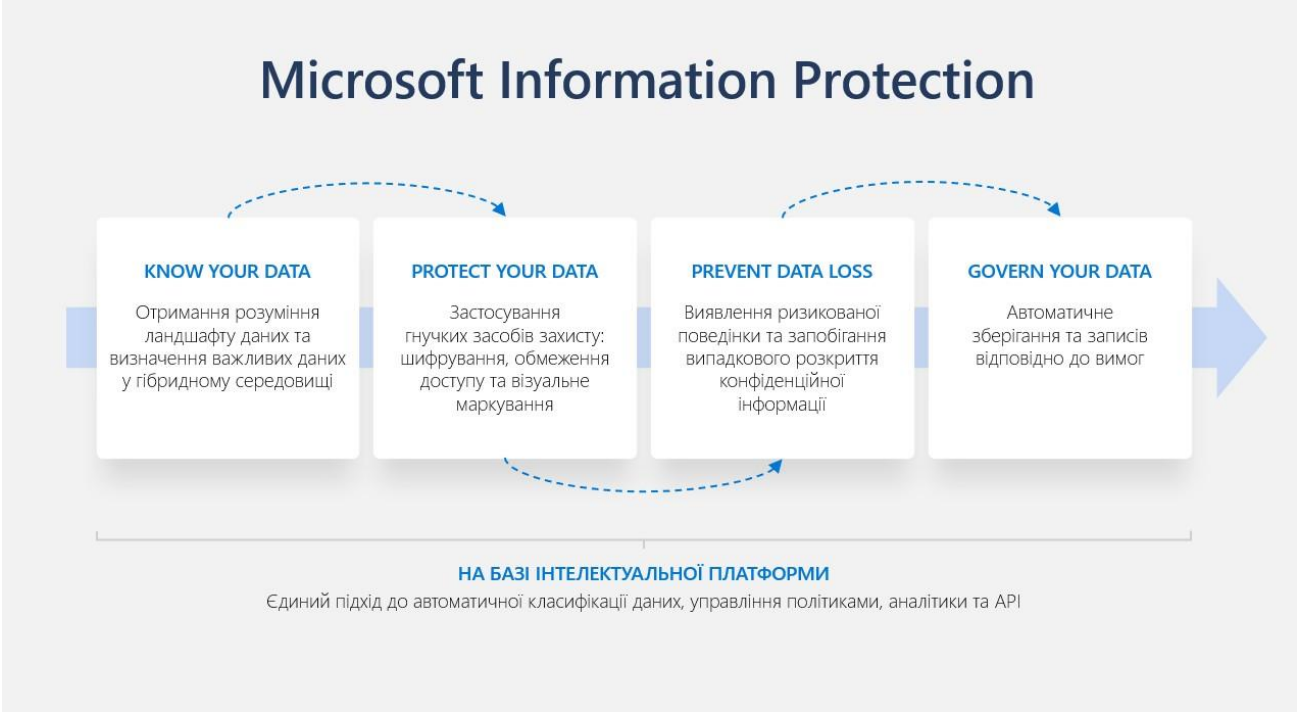


Рисунок 1.9 Microsoft Information Protection

Усю інформацію, доступну в компанії, необхідно спочатку класифікувати, щоб ідентифікувати конфіденційні дані, визначити, де вони знаходяться і які групи користувачів мають до них доступ, а також централізовано керувати ними. Тегування використовується для застосування гнучких заходів безпеки, таких як шифрування, обмеження доступу та візуальне маркування. Також необхідно визначити, яка інформація надається

виключно для внутрішнього користування, а яка є конфіденційною, щоб запобігти її випадковому витоку за межі компанії. Для цього слід використовувати функціонал сервісу Data Loss Prevention (DLP).

1.2.3.5 Захист пошти

Ми розглянемо комплексний підхід для захисту пошти з урахуванням найбільш поширених вразливостей. Якщо в компанії використовують пошту Exchange online, вона за замовчуванням включає хмарну службу Exchange online protection.

Це перша ланка фільтрації пошти, яка захищає вашу компанію від спаму, шкідливих програм та інших загроз електронної пошти. Але є ризик отримання листів зі шкідливими посиланнями або вкладеннями, тому я рекомендую організувати додатковий рівень захисту за допомогою Microsoft Defender for office 365. Для цього необхідно використовувати Microsoft Defender for office 365 Plan 1, яка включає розширені можливості запобігання загроз, наприклад, безпечні посилання — safe link, та безпечні вкладення — safe attach.

Safe Link сканує URL-адреси, щоб захистити вашу компанію від шкідливих посилань, які використовуються у фішингових та інших атаках.

Safe attach — функція, що забезпечує додатковий рівень захисту для вкладень електронної пошти перед їхньою доставкою одержувачам, а також допомагає захистити організацію від непередбаченого обміну шкідливими файлами в SharePoint, OneDrive та Microsoft Teams.

Як ваші співробітники будуть поводитись, якщо кіберзлочинці спробують дізнатися їх особисті дані або надішлють e-mail із запитом перейти за посиланням? Часто зловмисники діють через людей і використовують скомпрометовані адреси для розповсюдження шкідливого ПЗ.

Зі співробітниками треба проводити тренінги та виконувати симуляції фішингових атак, щоб подивитися на їхню поведінку. Можна найнятисторонню компанію для цього або зробити подібну симуляцію самостійно за допомогою Microsoft Defender for Office 365 — такий функціонал є у Plan2. Подібні тренінги підвищать рівень свідомості співробітників, їхньої підготовленості, здатності розпізнавати шкідливі повідомлення та не реагуватина них.

1.2.3.6 Application: виявлення потенційно небезпечних програм

Щоб зрозуміти, якими програмними системами користуються ваші співробітники, і чи є вони надійними та безпечними, вам потрібно використовувати Microsoft Defender для хмарних додатків. Рішення забезпечує повний контроль над конфіденційними даними завдяки комплексному моніторингу, аудиту та детальному контролю.

Microsoft Defender для хмарних додатків містить інструменти, які допомагають виявляти та оцінювати тіньові IT-ресурси, застосовувати політики безпеки та проводити розслідування інцидентів.

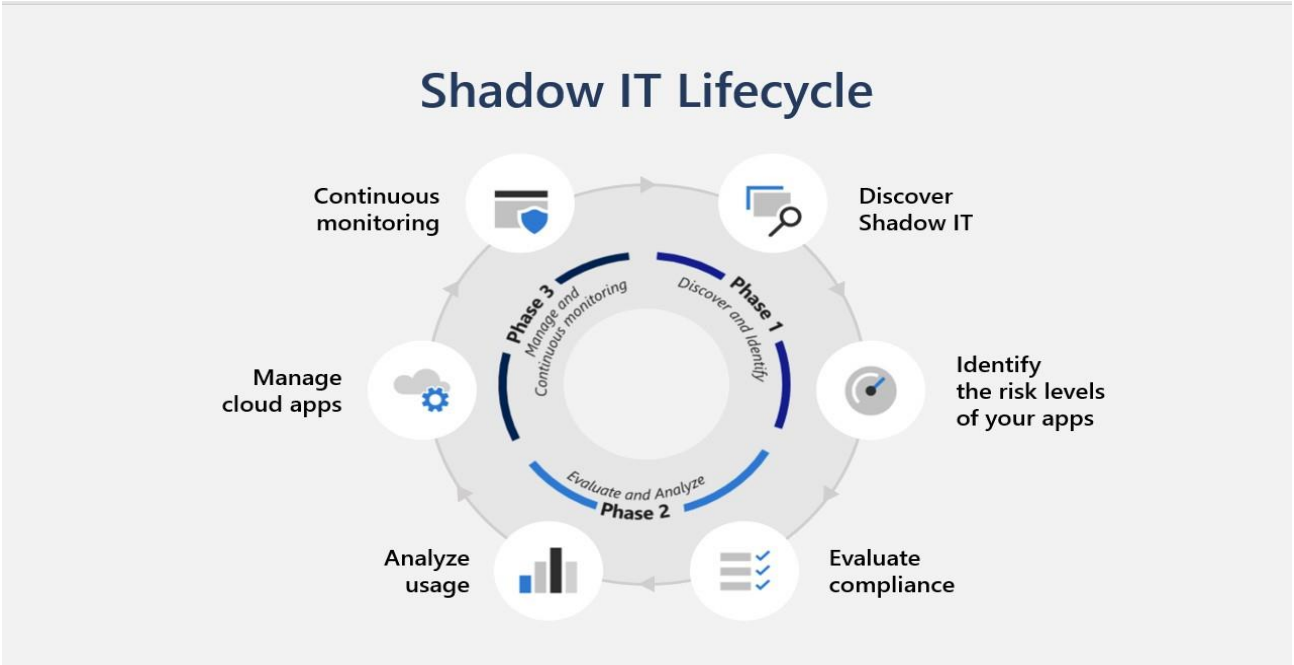


Рисунок 1.10 Shadow IT Lifecycle

1.2.3.7 Infrastructure: організація безпечної роботи в хмарі

Інфраструктура підприємства є критичним вектором загроз Microsoft Defender для хмарних технологій - це платформа управління хмарною безпекою та платформа захисту хмарних робочих навантажень для ресурсів Azure.

Microsoft Defender для хмарних технологій також може захищати більше робочих процесів для хмарних платформ, таких як Amazon Web Services (AWS) і Google Cloud Platform (GCP).

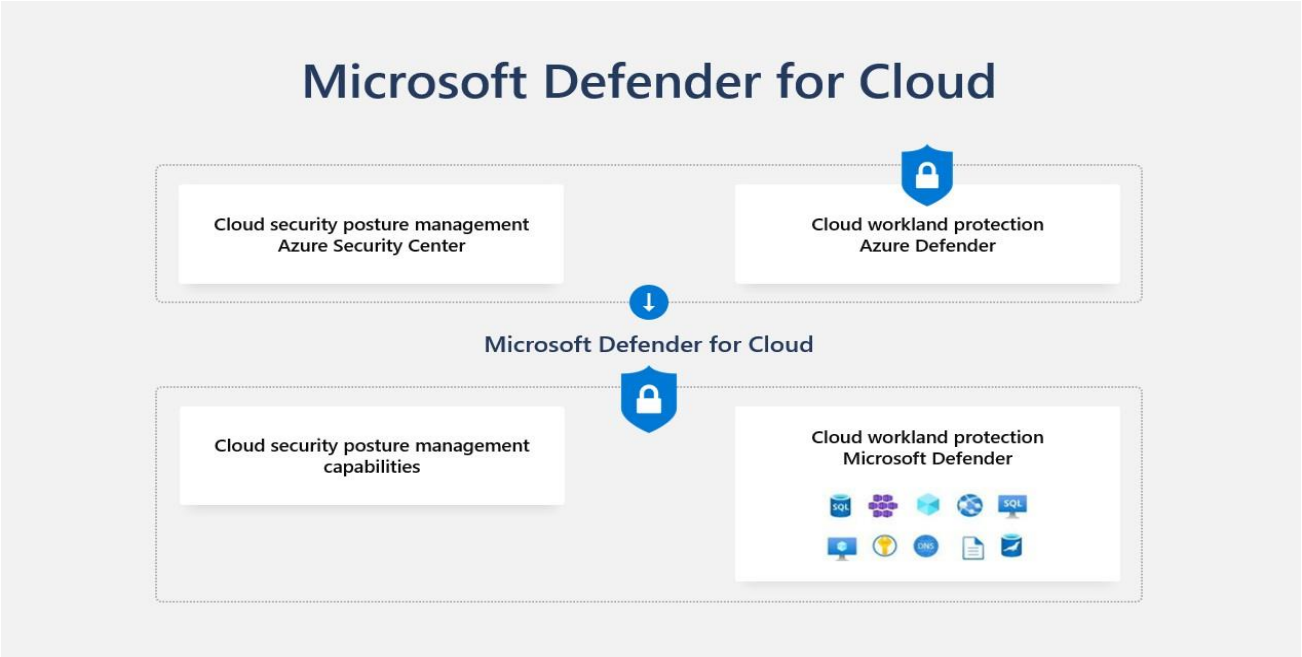


Рисунок 1.11 Microsoft Defender для хмарних технологій

Тобто у сучасної, прогресивної компанії, яка використовує хмарні технології по моделі multi-cloud, є можливість централізовано, з однієї консолі моніторити та налаштовувати політики безпеки.

1.2.3.8 Network: безпечний доступ до корпоративної мережі

Мережева безпека- це вже не просто обмеження зовнішнього доступу. Вона вимагає шифрування всіх зовнішніх і внутрішніх каналів зв'язку,

обмеження доступу на основі політик, мікро сегментації мережі та виявлення загроз у реальному часі.

Для цього у Microsoft розроблено цілий ряд продуктів, наприклад:

Azure Firewall-хмарний брандмауер для захисту віртуальних мережевих ресурсів Azure, розгортається за лічені хвилини, запобігає поширенню шкідливого програмного забезпечення, забезпечує аналіз внутрішнього та зовнішнього трафіку в режимі реального часу та легко масштабується.

Захист від DDoS - Адаптивна розвідка загроз автоматично відстежує та усуває DDoS-атаки, а також очищає трафік на периметрі мережі до того, як DDoS-атака вплине на програми та сервіси.

Microsoft також пропонує інші рішення для забезпечення мережевої безпеки, пристосовані до конкретних потреб компанії.

1.3 Аналіз кібератак на ланцюг поставок

Слабкою ланкою у кібербезпеці вашого підприємства можуть бути ваші партнери та постачальники. Ви можете скільки завгодно посилювати захист ваших IT-систем, але через атаку на зовнішню компанію хакери можуть отримати доступ до ваших даних.

Саме Supply chain attack стає однією з найнебезпечніших кіберзагроз, з якою доводиться мати справу Україні від початку повномасштабної війни. Хоча цей вид атак застосовувався і раніше.

1.3.1 Supply chain attack

Supply chain attack, або атака на ланцюг постачання, — це кібератака, під час якої хакери проникають в IT-системи компанії через зовнішнього партнера або постачальника (рис.1.12).

Головна загроза в тому, що компанії налагоджують потужний кіберзахист своїх інформаційних систем, але водночас їм важко контролювати всіх своїх партнерів та підрядників, яким дають доступ до своїх даних. Ці підприємства можуть мати нижчий рівень кіберграмотності серед співробітників, слабші рішення з кібербезпеки тощо. Саме цими вразливостями хакери й користуються, атакуючи компанії-підрядники та отримуючи доступ до потрібних їм інформаційних систем.

Чому компанії, які є ціллю для хакерів, атакують через підрядників:

- Сама цільова компанія надійно захищена від зовнішніх атак і втручання напряму реалізувати неможливо.
- Підрядна організація має нижчий рівень розвитку кібербезпеки, ніж цільова компанія.
- Цільова компанія має підрядників із легітимними доступами до своїх систем.

Рисунок 1.12 Анализ атаки через компанію-підрядника

1.3.2 Приклади кібератак на ланцюг постачання

Supply chain attack стали активно застосовуватися по всьому світу останні кілька років. У 2019-му Symantec наголосила, що кількість цих атак зросла на 78% у порівнянні з 2018-м. А вже у 2021-му саме безпеку ланцюгів постачання уряди та політики висунули на перший план у США.

Одним із показових прикладів стала масштабна Supply chain-атака на розробника програмного забезпечення SolarWinds у 2020 році. Вона вразила сотні найбільших компаній США, а також підприємства у Північній Америці, Європі та Азії. Отже, що сталося?

Група хакерів (вважають, що це була російська Cozy Bear) скомпрометувала оновлення програмного забезпечення Orion від SolarWinds. Цей доступ зловмисники використали, щоб створити та поширити троянські оновлення серед користувачів ПЗ.

Виявилося, що так хакери отримали доступ до інформаційних систем, що належать багатьом компаніям зі списку Fortune 500 та американським урядовим департаментам, зокрема Міністерству фінансів і торгівлі США. Під удар потрапили десятки провідних телекомунікаційних компаній, п’ять провідних бухгалтерських фірм, усі гілки збройних сил США, Пентагон, атакож сотні університетів і коледжів по всьому світу.

Ось ще кілька прикладів атак на ланцюг постачання:

- ASUS, 2018 рік. Хакери скористалися функцією оновлення та поширили вірус на 500 тисяч систем.
- British Airways, 2018 рік. Розділ платежів на сайті British Airways містив код, який збирав платіжні дані клієнтів та спрямовував їх на шахрайський сайт. Так зловмисники отримали інформацію про приблизно 500 тисяч клієнтів компанії.
- Mimecast, 2021 рік. Під час атаки хакерам вдалося скомпрометувати сертифікат безпеки, який підтверджує автентифікацію служб

Mimecast у сервісах Microsoft 365 Exchange. Це вплинуло на 10% клієнтів Mimecast.

- Colonial Pipeline — найбільша американська трубопровідна система. Доставляє бензин, дизпаливо та авіагас із Техасу до Нью-Йорка. Забезпечує майже 45% палива для східного узбережжя США. В результаті зафіксованої 7 травня 2021 року атаки трубопровідна система Colonial Pipeline зупинилася, у США оголосили регіональний надзвичайний стан. Заінформацією у ЗМІ, за день до атаки з серверів компанії кіберзлочинці викрали 100 Гб даних.

Приклад Supply chain-атаки добре відомий українцям з 2017 року: вірус NotPetya, який шифрував файли на жорсткому диску комп'ютера-жертви, перезаписув і шифрував MBR-дані, щоб унеможливити завантаження операційних систем комп’ютерів. Зловмисники вимагали викуп у біткоїнах, проте навіть його сплата не допомагала відновленню систем. Тому була версія, що викуп не справжня мета атаки.

В результаті запуску NotPetya відбулося масове блокування роботи багатьох українських державних підприємств, установ, банків, медіа тощо, зокрема аеропорту «Бориспіль», ЧАЕС, Укртелекому, Укрпошти, Ощадбанку, Укрзалізниці та інших підприємств критичної інфраструктури. Також були вражені урядові цифрові інфраструктури, зокрема Кіберполіція та Служба спецзв'язку. Усі ці ресурси були атаковані за рахунок компрометації популярних сервісів компанії M.E.Doc, яке відбулось значно раніше того ж року.

1.3.3 Supply chain-атака в Україні під час війни та захист від них

Через повномасштабне вторгнення рф в Україну майже кожен бізнес став жертвою кіберзлочинців. Водночас зараз саме Supply chain-кібератака є однією з найбільших загроз для компаній-критичних об’єктів, які співпрацюють із підрядниками і можуть бути ціллю хакерів. Зокрема, для

урядових структур, банківської сфери, виробництва, підприємств критичної інфраструктури тощо.

Компанії-замовники під час війни часто мають більше ресурсів, щоб залишатися стабільними. Водночас компанія-підрядник маленька. Будь-яка зміна більше впливає на процеси в ній, зокрема міграція співробітників, військові дії, мобілізація тощо. На практиці співробітник підрядної організації, який має доступ до мережі замовника, може під час сирени піти у бомбосховище. Через свій емоційний стан він може в цей час не перервати робочу сесію, чим одразу скористаються зловмисники. Хакери вичікують такі моменти, щоб отримати легальний доступ до мережі цільового підприємства.

Рисунок 1.13 Фактори сбільшеня ризиків Supply chain attack

Різниця між кібератаками у мирний час та під час війни у тому, що змінюється мета злому. Зазвичай хакери блокують доступ до даних і вимагають за них викуп. Натомість мета атаки у воєнний час — отримати доступ до критично важливих даних, знищити критичну інфраструктуру і таким чином завдати непоправної шкоди противнику. Саме тому компаніям варто напрацювати жорсткі політики роботи з третіми сторонами.

Як захистити постачальників та партнерів від кібератак?

Підприємствам-замовникам, особливо критично важливих об’єктів,варто розуміти, що периметр кібербезпеки компанії не завершується лише на власній інфраструктурі. Він завжди розширюється на партнерів та підрядників, які мають легітимний доступ до IT-систем замовника.

Ось кілька кроків, як протидіяти Supply chain-атакам, які рекомендує директор з кібербезпеки "Київстар" Юрій Прокопенко, спираючись на власний досвід:

1. Посилення контролю підрядних організацій, зокрема контролю обладнання, з якого з вами працюють їхні співробітники.
2. Вимоги до підрядників щодо гарантування високого рівня кібербезпеки у власній інфраструктурі, а також проходження ними незалежного аудиту.
3. Розгляд можливості надавати підрядним організаціям сервіс для гарантованого кіберзахисту IT-систем.

Рисунок 1.14 Заходи протидії Supply chain attack

Водночас самим підрядним організаціям варто приділити більшу увагу внутрішньому контролю — захисту робочих точок і серверного обладнання, навчанню співробітників кібергігієні та кібербезпеці.

2 ОХОРОНА ПРАЦІ

Вступ

Згідно з ч. 1 ст. 13 Закону України «Про охорону праці» роботодавець зобов'язаний створити на робочому місці в кожному структурному підрозділі умови праці відповідно до нормативно-правових актів, а також забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ЕОМ. Велике значення має раціональна конструкція і розташовує елементів робочого місця, що важливе для підтримки оптимальної робочоїпози людини-оператора. В процесі роботи з комп'ютером необхідно дотримувати правильний режим праці і відпочинку.

Дотримання норм охорони праці є спільним завданням як роботодавця, так і працівника. У вирішенні питань з охорони праці можна звернутися до законодавства України з охорони праці.

Метою данного розділу дипломного проекту є визначення оптимальних умов праці програміста та обов`язків з охорони праці..

1.Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу

На робочому місці розробника програмного забезпечення: підвищений рівень отримуваного електромагнітного випромінювання, статична електрика, високий рівень шуму, несприятливі умови мікроклімату, підвищена напруга на зір та мозок тощо.

Під час робочого процесу програміст піддається впливу великої кількості шкідливих та небезпечних факторів, а саме: шуми, вібрації, інфрачервоне випромінювання, електромагнітне випромінювання, електричний

струм, емоційне та нервове навантаження, сидяче положення тіла протягом дового часу. Тому дуже важливо забезпечити правильний нормований графік та організувати робочий процес так, щоб мінімізувати вплив усіх перелічених раніше небезпечних та шкідливих факторів.

2 Гігієнічні вимоги до виробничого середовища.

Вимоги, що пред'являються до умов праці на виробництві, визначаються необхідністю забезпечення таких умов праці на робочому місці, при яких виключено несприятливий вплив на працездатність і здоров'я працюючих і можуть бути забезпечені оптимальні границі поділу і кооперації праці, а в кінцевому підсумку підвищення ефективності та якості праці.

2.1 Вимоги до приміщення

Обємно-планувальні рішення будівель та приміщень для роботи з ВДТ мають відповідати вимогам ДСанПІН 3.3.2.007-98. Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Площа на одне робоче місце становить не менше 6,0 м^2, а об’єм – не менше ніж 20,0 м^3. У приміщеннях слід щоденно робити вологе прибирання. Вони повинні бути оснащені аптечками першої медичної допомоги. При приміщеннях мають бути обладнанні побутові приміщення для відпочинку.

Для стін і робочих поверхонь використовують мало насичені (основні) кольори, для невеликих помешкань або ділянок, що рідко потрапляють у поле зору працюючих, а також для створення контрастності – кольори середньої насиченості (допоміжні), для маленьких по площі поверхонь – насичені (акценти) – як функціональне фарбування. Стелі у всіх приміщеннях повинні бути білими. Поверхні устаткування в приміщеннях повинні бути матовими або напівматовими для виключення випадку відблисків світла в очі працюючого, а стіни бути пофарбованими фарбами пастельних тонів.

2.2 Освітлення

Відповідність характеристик систем освітлення нормативним вимогам гарантує не тільки збереження здоров'я, а й високі продуктивність і якість праці. На підприємствах використовується природне і штучне освітлення. Перше призначено для роботи в денний час, а друге - у вечірній, коли природного освітлення недостатньо. Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення, відповідно до ДБН В.2.5-28:2018 « Природне і штучне освітлення».

Для штучного освітлення у приміщенні використовуються люмінесцентні лампи типу ЛБ, які в порівнянні з лампами розжарювання мають ряд істотних переваг: за спектральним складом світла вони близькі до природного світла, мають підвищену світлову віддачу (у 2-5 разів вищу, ніж у ламп розжарювання); мають триваліший термін служби – до 10 тис годин.. Допускається застосування ламп розжарювання у світильниках місцевого освітлення.

2.3 Шум

Рівні шуму та вібрації на робочих місцях осіб, що працюють з ПК, визначаються відповідно до ДСанПіН 3.3.2.007-98.

Для забезпечення дотримання допустимих рівнів шуму на робочих місцях застосовуються засоби звукопоглинання, вибір яких обґрунтовується спеціальними інженерно-акустичними розрахунками (п. 3.3.3 ДСанПіН 3.3.2.007-98).

2.4 Мікроклімат

У виробничих приміщеннях на робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносноївологості й рухливості повітря – ДСН 3.3.6.042-99 «і норми мікроклімату виробничих приміщень».

Параметри мікроклімату значення параметрі

Взимку влітку

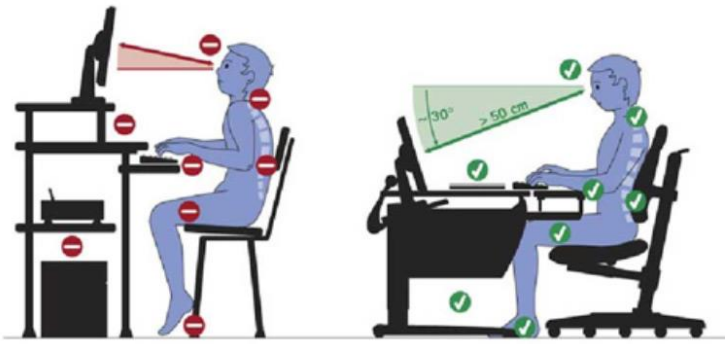
Температура, C^0	22-24	23-25
Відносна вологість, %	40-60	40-60
Швидкість руху повітря, м/с	0,1	0,1-0,2

Нормалізація параметрів мікроклімату у виробничих приміщеннях здійснюється за допомогою систем опалення. Ці системи поділяються на водяні парові та повітряні. Кількість теплоти, що генерується системою опалення, має відповідати втрат теплоти в приміщенні (через будівельні конструкції, на нагрів повітря в приміщенні, технологічні тепловтрати, нагрів надходять матеріалів і напівфабрикатів). Основними засобами захисту від теплових випромінювань є екранування та теплоізоляція, а також пристрій місцевих припливних систем вентиляції. При природній вентиляції (за допомогою вікон) повітря надходить у приміщення і видаляється з нього внаслідок різниці температур і тиску.. Механічна вентиляція забезпечується вентиляторами, що забирають повітря зовні і направляє його до будь-якого робочого місця. або устаткування, а також видаляють забруднене повітря

2.4 Вимоги до організації робочого місця працівника

До самостійної роботи на комп'ютерах допускаються особи, які пройшли медичний огляд, навчання по професії, вступний інструктаж з охорони праці та первинний інструктаж з охорони праці на робочому місці. В подальшому вони проходять повторні інструктажі з охорони праці на робочомумісці один раз на півріччя, періодичні медичні огляди один раз на два роки

Робочі місця повинні бути розташовані так, щоб у поле зору працюючого не попадали поверхні, що мають властивість віддзеркалювання, вікна освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90-100 градусів від вікон, так, щоб світло падало з боку. Робочі місця з ВДТ доцільно розміщати в глибині приміщення. Розташування відео термінала, при якому працюючий звернений обличчям або спиною до вікон, неприпустимо при будь-якому способі реалізації загального висвітлення, як прямим, так і відбитим світлом.



Робочий стіл повинен регулюватися по висоті в границях 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля Рекомендовані розміри столу: висота 725 мм, ширина 600-1400 мм, глибина 800-1000 мм. Робочий стілець повинен бути оснащений підйомно-поворотним пристроєм для регулювання висоти сидіння і спинки, а також кута її нахилу. Регулювання кожного параметра повинне вироблятися легко, бути незалежним і надійно фіксуватися.

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом $+30^0$ до нормальної лінії погляду працюючого.

Клавіатуру слід розташовувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого.

3 Пожежна безпека

Під пожежною безпекою розуміють систему державних і суспільних заходів, спрямованих на охорону від вогню людей і власності. Пожежна безпека приміщень, що мають електричні мережі, регламентується ГОСТ 12.1.033-81, ГОСТ 12.1.004-85. Робота оператора ЕОМ повинна вестися в приміщенні, що відповідає категорії Д пожежної безпеки (негорючі речовини
й матеріали в холодному стані).

Куріння у не відведених для цього місцях	Порушення правил користування електроприладами	Необережне поводження з вогнем

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 приступити до ліквідації пожежі.

ВИСНОВКИ

У кваліфікачійній роботі був проведен аналіз методів та засобів інформації безпеки українського ІТ-бізнесу та виявлено, що існує безліч інструментів та методів захисту, які можуть бути використані для запобігання кібератакам різного рівня. Було проаналізовано комплексної ІТ-безпеки компанії - на прикладі інструментів Microsoft також було проаналізовано Supply chain-атака в Україні під час війни та захист від них.

Аналіз показав, що проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства. З огляду на сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково- технічних, організаційних та просвітницьких напрямів конструюванняефективної системи кіберзахисту у рамках комплексної протидії кіберзагрозам сприятиме формуванню ефективного механізму протидії загрозам у кібернетичній сфері, випереджальному реагування на динамічні зміни, що відбуваються у кіберпросторі, розробленню та впровадження ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 17799:2005. Informationtechnology. Security techniques. Code ofpracticeforinformationsecuritymanagement.
2. ISO/IEC 27001:2005. Informationtechnology. Security techniques. Informationsecuritymanagementsystems. Requirements.
3. ISO/IEC TR 27035:2011. Informationtechnology − Security techniques − Informationsecurityincidentmanagement.
4. ISO/IEC 20000:2011. Informationtechnology. Servicemanagement. Part 2: Code ofpractice.
5. DefiningIncidentManagementProcessesforCSIRTs: A WorkinProgress // CMU/SEI-2004-TR-015: ESC-TR-2004-015 ChrisAlberts, AudreyDorofee, GeorgiaKillcreceOctober 2004 NetworkedSystemsSurvivabilityProgram.
6. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 2 (92). – С.53-56.
7. Гавриленко О.В. Відповідність національної нормативної бази у сфері технічного захисту інформації міжнародним стандартам: зіставлення документів, шляхи гармонізації. Матеріали XVII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м.Київ, 2015.
8. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”. [Електрон. ресурс]: –Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835.
9. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31. – с.286

10. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. [Електрон. ресурс]: – Режим доступу: http://www.uk.xlibx.com/4yuridicheskie/1354389-1-sou-nbu-651-suib-10-2010-standart-organizacii-ukraini-nastanova-metodi-zahistu-bankivskiy-diyalnosti-siste.php.

11. НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”. [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

12. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

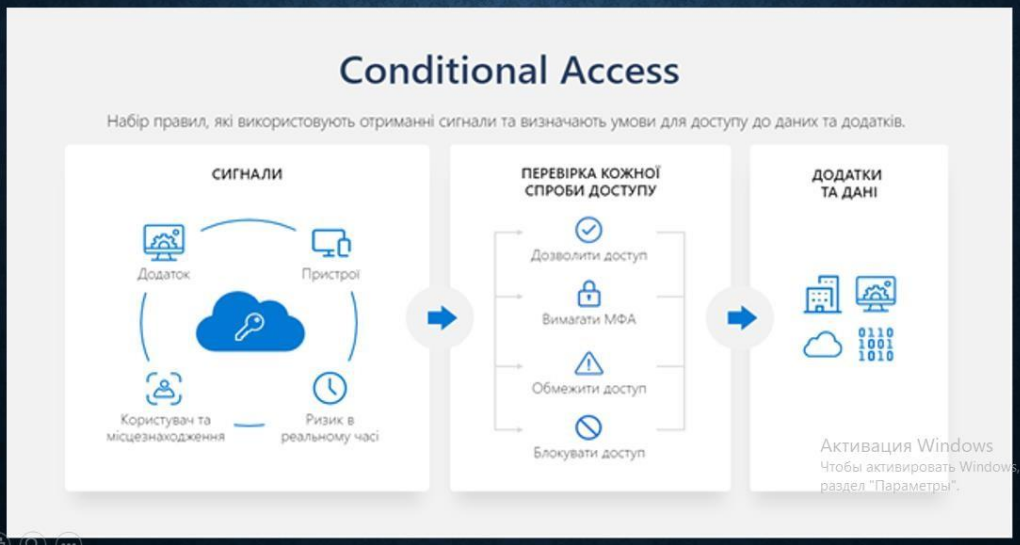
ДОДАТОК А

Слайди мультимедійної презентації

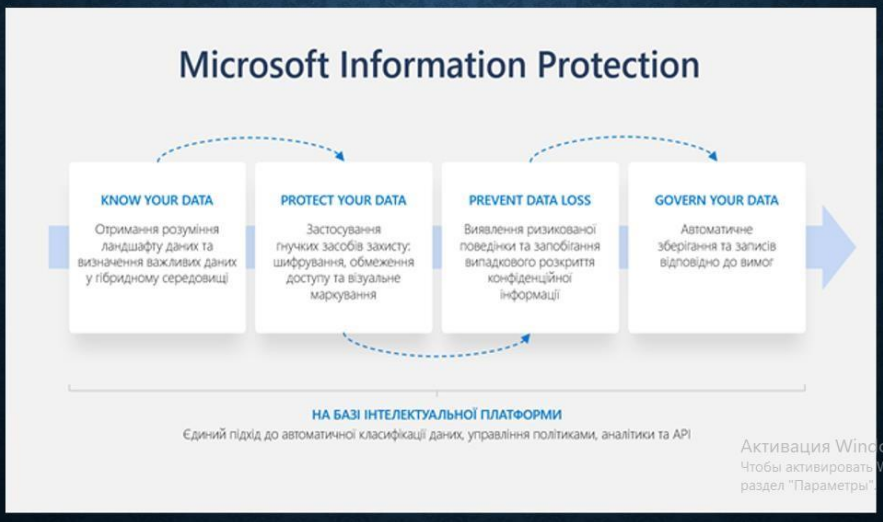
Система інформаційного контролю IT-компанії

ПРИНЦИП ДІЇ MFA

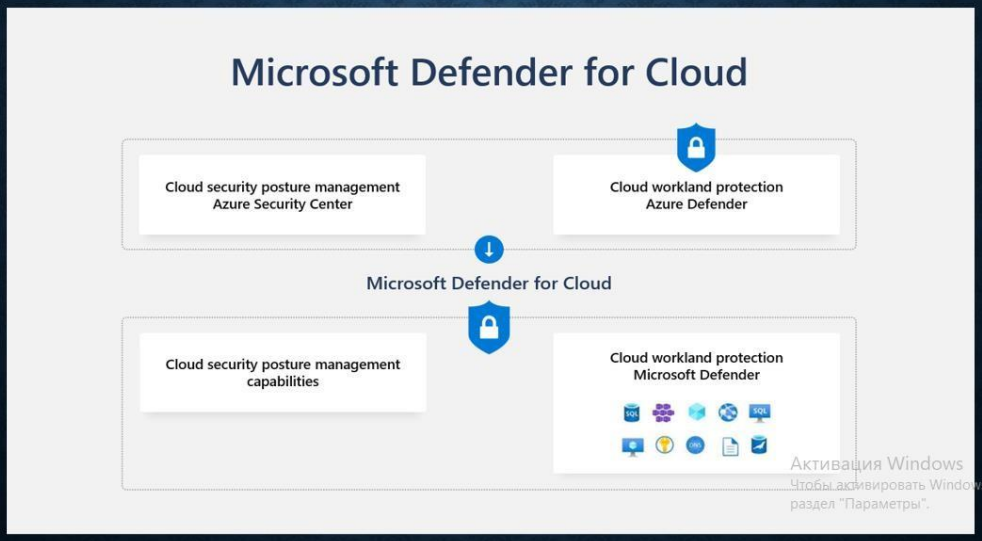
НАБІР ПРАВИЛ УПРАВЛІННЯ ДОСТУПОМ CONDITIONAL-ACCESS



Безпечна робота з корпоративними даними



MICROSOFT DEFENDER ДЛЯ ХМАРНИХ ТЕХНОЛОГІЙ



Анализ атаки через компанію-підрядника

ФАКТОРИ СБІЛЬШЕНЯ РИЗИКІВ SUPPLY CHAIN ATTACK

ЗАХОДИ ПРОТИДІЇ SUPPLY CHAIN ATTACK

UNICHECK
by Turnitin

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015625297

Дата перевірки:
16.06.2023 12:43:29 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
16.06.2023 12:47:16 EEST

ID користувача:
100011688

Назва документа: **2БКС-27 Поляков І.Д.**

Кількість сторінок: **40** Кількість слів: **7490** Кількість символів: **59471** Розмір файлу: **908.69 KB** ID файлу: **1015272202**

20.3%
Схожість

Найбільша схожість: **7.4%** з Інтернет-джерелом (https://legalitgroup.com/bezpeka-it-kompaniyi-riziki-zahist-zahist-it-ko..

20.3% Джерела з Інтернету	345	Сторінка 42

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	1

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на випускну роботу бакалавра здобувача освіти
відділення комп'ютерних систем

Полякова Іллі Дмитровича

(прізвище, ім`я та по батькові)

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

Освітня програма **Обслуговування комп'ютерних систем та мереж**

Керівник дипломного проекту (роботи) **Шевцов Юрій Сергійович**

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи)

Аналіз методів та засобів інформаційної безпеки українського IT-бізнесу

Обсяг розрахунково-пояснювальної записки 66 сторінок

Обсяг графічної (презентаційної) частини 12 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Дипломний проект повністю відповідає завданню до дипломного проектування. Графічна частина складається з окремих слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра.

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Пояснювальна записка дипломного проекту виконана якісно, у повному обсязі. В дипломному проекті здобувачем проаналізовано методи та засоби інформаційної безпеки українського IT-бізнесу. Розглянуті технічні та програмні методи. В дипломному проекті в останніх розділах проаналізовано економічні показники та питання охорони праці.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) _____

Презентаційні матеріали виконані якісно, демонстративно та відповідають вмісту теоретичного матеріалу

г) перелік позитивних якостей дипломного проекту (роботи)_____

Здобувачем проаналізовані методів та засобів інформаційної безпеки українського ІТ-бізнесу, що є дуже актуальною тематикою в наш час. Розглянуті технічні та програмні методи та засоби інформаційної безпеки які пропоновані до використання в Україні.

д) основні недоліки дипломного проекту (роботи) _____

Серед недоліків роботи варто вказати, відсутність посилань на перелік використаних джерел та наявність орфографічних помилок в тексті пояснювальної записки

Оцінка розрахункової частини _____ *Добре*

Оцінка графічної частини _____ *Добре*

Загальна оцінка _____ *Добре*

Прізвище, ім'я, по батькові рецензента _____ *Василіу Євген Вікторович*

Місце роботи і посада рецензента *Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ, декан факультету інформаційних технологій та кібербезпеки*

Підпис: _____

«16» 06 2023 р.

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ ДУІТЗ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ * 43997335 * ВІДДІЛ КАДРІВ

ВСП «Одеський технічний фаховий коледж ОНТУ»

ВІДГУК

керівника про випускну роботу бакалавра

Полякова Іллі Дмитровича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Тема випускної роботи Аналіз методів та засобів інформаційної безпеки українського ІТ-бізнесу

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки) Випускна робота виконана відповідно технічному завданню. Пояснювальна записка до випускної роботи містить 66 сторінок. У пояснювальній записці зроблено аналіз методів та засобів інформаційної безпеки українського ІТ-бізнесу, які розділяються на технічні та програмні. Графічна частина складається з 12 слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра, розробку виконано на 90%.

б) Самостійність роботи

Протягом виконання випускної бакалаврської роботи Поляков І.Д. поступово та послідовно виконував всі етапи, проявив ініціативу у створенні загальної концепції та реалізації випускної роботи. Всі роботи він виконував самостійно, з оглядом на рекомендації керівника.

в) Теоретична підготовка здобувача освіти

Поляков І.Д. під час роботи над випускною бакалаврською роботою вивчив достатню кількість літературних джерел за даною тематикою.

Вважаю, що теоретична підготовка здобувача освіти добра і він готовий до захисту роботи.

г) Вміння розв`язувати виробничі і конструкторські питання на базі останніх досліджень науки і техніки, передових методів виробництва

Під час виконання роботи Поляков І.Д. мав змогу самостійно приймати окремі рішення з виконання програмної частини роботи та показав вміння організовано працювати над поставленою задачею, користуючись сучасними комп'ютерними програмними засобами.

Оцінка розрахункової частини Добре

Оцінка графічної частини Добре

Загальна оцінка Добре

Прізвище, ім`я, по батькові Харченко Роман Юрійович к.т.н.

Місце роботи і посада керівника роботи

доцент каф. "Морського радіозв'язку" НУ «Одеська Морська академія»

Підпис

«____» _____ 20___ р.

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

Ми, що нижче підписалися,

Поляков Ілля Дмитрович,
здобувач освіти гр. 2БКС-27, та

Харченко Роман Юрійович,
керівник дипломного проекту,

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

«Аналіз методів та засобів інформаційної безпеки українського IT-бізнесу»
(автор роботи – Поляков І.Д., керівник роботи – Харченко Р.Ю.)

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 _____ / Поляков І.Д. /

Керівник _____ / Харченко Р.Ю./

« 12 » _____06_____ 2023 р.