Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра інформаційно-документних комунікацій

ЗАТВЕРДЖУЮ
на засіданні кафедри
інформаційно-документних комунікацій
(протокол № __від_____2024 р.)
Завідувач кафедри _____ Ганна ОХРІМЕНКО

Кваліфікаційна робота
на здобуття освітнього ступеня бакалавра
на тему:

«Захист інформації від несанкціонованого доступу у контексті аналітичної культури організації в Україні: регіональний аспект»

Виконала студентка IV курсу, групи Інс-41
спеціальності 029 «Інформаційна, бібліотечна та архівна справа»
Фрідріх Поліна Андріївна

Керівник – кандидат історичних наук,
доцент кафедри інформаційно-
документних комунікацій
ОХРІМЕНКО Ганна Валеріївна
Рецензент – доктор філософії з
педагогічних наук, старший викладач
ФЕДОРУК Олеся Михайлівна,

Острог, 2024

Графік виконання кваліфікаційної роботи на першому (бакалаврському) рівні вищої освіти

№ п/н	Види та етапи робіт	Термін виконання	Підпис наукового керівника
1	2	3	4
1	Вибір теми, закріплення її на кафедрі та визначення наукового керівника	Вересень-жовтень 2023-2024 н.р.	
2	Складання графіка роботи над темою і узгодження його з науковим керівником	Жовтень-листопад 2023-2024 н.р.	
3	Вивчення джерел, літератури, суспільних реалій, матеріалів архівів, періодичних видань; збір та узгодження фактів, даних	Листопад-грудень 2023-2024 н.р.	
4	Складання плану кваліфікаційної роботи й узгодження його з науковим керівником	Грудень 2023-2024 н.р.	
5	Формування концепції, написання вступу й теоретичного розділу роботи	Січень-лютий 2023-2024 н.р.	
6	Написання дослідницької частини кваліфікаційної роботи	Лютий-квітень 2023-2024 н.р.	
7	Завершення рукопису кваліфікаційної роботи та ознайомлення наукового керівника з її першим варіантом	Квітень-травень 2023-2024 н.р.	
8	Повне завершення кваліфікаційної роботи, оформлення її та подання на відгук наукового керівника	Травень 2024 року	
9	Подання роботи на кафедру	до 15 травня 2024 року	
10	Проведення попереднього захисту	до 18 травня 2024 року	
11	Подання рецензії на кафедру	до 12 червня 2024 року	
12	Захист кваліфікаційної роботи	19-20 червня 2024 року	

Здобувач першого (бакалаврського)

рівня вищої освіти **_____ Фрідріх Поліна**

Науковий керівник **_____ Охріменко Ганна**

ЗМІСТ

ВСТУП

Актуальність теми дослідження.

В сучасному світі відбувається стрімкий перехід від типової промислової роботи до інформатизації всіх сфер суспільства, наслідком якого є розвиток інформаційних технологій та процесів. Несучи в собі багато користі, такої як прозорість інформації та реалізацію інформаційних запитів користувачів, ці процеси також можуть використовуватися в негативному контексті, допускаючи зловживання певною інформацією в цілях завдання шкоди певним громадянам, організаціям, державам.

В часи боротьби за лідерство у сферах науки, економіки, військової оборони - захист інформації є провідною складовою безпеки в Україні. Її актуальність зумовлена високою чисельністю інформаційних загроз та кібератак на державні та приватні установи, які займаються аналітикою.

Щоб ефективно використовувати зібрані показники, необхідно побудувати всередині організації їх збирання, обробку та зберігання. Крім того, важливо захищати ці дані, забезпечуючи їхню конфіденційність, цілісність та доступність при подальшій роботі.

Актуальність теми «Захист інформації від несанкціонованого доступу у контексті аналітичної культури організації в Україні», ґрунтується на необхідності подальшого розвитку захисту інформації аналітичних установ, від несанкціонованого доступу та різноманітних внутрішніх та зовнішніх загроз.

Описуючи кожен етап становлення та розвитку системи захисту інформації обмеженого доступу в Україні, ми визначаємо основні досягнення, які лягли в основу розвитку цієї важливої галузі та можуть розглядатися як основа для подальших напрямів удосконалення системи обмеженого доступу нашої країни.

Стан наукової розробленості теми.

Для написання роботи було опрацьовано роботи науковців в галузі інформаційного права, захисту інформації та аналітичної культури: І. Л. Бачило,

С. Л. Ємельянова, В. А. Копилова, Б. А. Кормича, Н.І. Логінова, А. І. Марущака, І. В. Смолякової, В. С. Цимбалюка, М. Я. Шевця та інших.

Важливу роль у написанні зіграли роботи «Правовий захист інформації» Н.І. Логінової, Р.Р. Дробожура, «Становлення й розвиток системи захисту інформації з обмеженим доступом в Україні» Д.В. Коца та «Захист інформації у контексті забезпечення інформаційної безпеки» М.В. Барана та практичний посібник «Корпоративна безпека» Ю.І. Когута.

Деякі науковці (О.В. Шапета та ін.) акцентують увагу на дослідженні становлення та розвитку систем захисту інформації, висвітлюючи це питання з точки зору аналітичної культури організації та аспектів, пов'язаних з нею. Проте досліджувані ними періоди охоплюють новітню історію нашої країни до 2005 року, що спонукає сучасних дослідників зосередити увагу на цій темі, та дослідити актуальніші періоди, а також регіони.

Мета дослідження.

Вивчити специфіку захисту інформації від несанкціонованого доступу в установах, які займаються аналітикою, а також виявити недосконалості їхніх систем захисту та запропонувати шляхи їх вдосконалення.

Завдання дослідження.

1. Дослідити поточний стан захисту інформації в організаціях України з регіональною спрямованістю.
2. Визначити основні загрози та вразливості, з якими стикаються організації в контексті захисту інформації.
3. Розробити стратегію захисту інформації, враховуючи особливості аналітичної культури в організаціях України.
4. Проаналізувати поточні методи та технології захисту інформації, використовувані в організаціях України, та їх ефективність.
5. Вивчити нормативну базу щодо захисту інформації в Україні та оцінити її відповідність вимогам сучасної аналітичної культури.
6. Вивчити існуючі стандарти та методики оцінки ризиків у сфері захисту інформації

7. Провести аналіз розвитку нових технологій та трендів у сфері захисту інформації, що можуть бути застосовані в регіональних організаціях.

8. Вивчити досвід інших країн щодо захисту інформації та перевести його в контекст України з урахуванням регіональних особливостей.

9. Провести тестування системи захисту інформації в досліджуваній організації та оцінити її ефективність.

Ці завдання допоможуть дослідити сучасний стан захисту інформації в регіональних організаціях України, розробити рекомендації щодо покращення системи захисту та врахувати аналітичну культуру в процесі захисту інформації.

Об’єкт дослідження.

Об’єктом дослідження в даній темі є аналітична культура організації в Україні. Це включає оцінку практик, ставлення та можливостей, пов’язаних з аналізом інформації та процесами прийняття рішень.

Предмет дослідження.

Предметом дослідження даної теми є захист інформації від несанкціонованого доступу. Він зосереджений на вивченні різноманітних заходів, стратегій і методів, які застосовуються організаціями в Україні для захисту своєї інформації від несанкціонованого доступу чи злому.

Територіальні та хронологічні межі дослідження

Хронологія дослідження описує період з 2005 року до сьогодення, а територіальні межі охоплюють сучасну Україну в цілому, в другому і третьому розділах увага акцентується на організаціях Київської та Львівської областей, які входять до групи компаній «Фокстрот».

Методологічна база дослідження

При дослідженні обраної теми був використаний метод теоретичного аналізу та синтезу наукових спостережень спеціалістів, які працюють в галузі безпеки інформаційних та комунікаційних систем, що дозволяє всебічно досліджувати тему, включаючи поглиблений аналіз організаційної культури та збір статистичних даних, пов’язаних із заходами інформаційної безпеки.

Також використовувався метод збору даних. Первинні дані були отримані за допомогою інтерв'ю з працівником департаменту інформаційних технологій другої лінії підтримки ТОВ «ЕНТРІ»– Олександром Робенком про аналітичну культуру та практики захисту інформації в організаціях в Україні. Вторинні дані включають галузеві звіти, організаційну політику та відповідні статистичні дані, які були надані керівником відділу служби безпеки групи компаній «Фокстрот» - Олексієм Пащенком під час інтерв'ю.

Наукова та практична значущість кваліфікаційної (дипломної) роботи.

Наукове значення

Дослідження робить внесок у наявний масив знань, надаючи розуміння взаємодії між інформаційною безпекою та аналітичною культурою. Це допомагає поглибити наше розуміння того, як організації в Україні можуть ефективно захищати свою інформацію від несанкціонованого доступу. Також дослідження може виявити різні фактори, які впливають на практику захисту інформації, такі як організаційна культура, регіональна динаміка та роль аналітики. Це розуміння може слугувати основою для подальших наукових досліджень і досліджень у цій галузі.

Результати цієї роботи можуть мати ширші наслідки за межами досліджуваних регіональних організацій. Вони можуть служити орієнтиром для інших установ, які прагнуть посилити свої заходи безпеки інформації, враховуючи культурний і регіональний контекст.

Практичне значення

Інформування про політику та нормативно-правові акти, як результати дослідження можуть дати цінну інформацію для розробників політики захисту та регуляторних органів в Україні. Вони можуть допомогти в розробці або вдосконаленні політики безпеки, враховуючи конкретні потреби та виклики організацій, що працюють у країні. У роботі також надані практичні рекомендації та найкращі практики для організацій в Україні щодо покращення заходів інформаційної безпеки.

Дослідження висвітлює ефективні стратегії, технології та підходи до захисту інформації від несанкціонованого доступу, сприяючи культурі безпеки в організаціях. Розуміючи зв’язок між аналітичною культурою та захистом інформації, організації можуть визначити потенційні вразливі місця та вжити заходів для пом’якшення ризиків.

Загалом впровадження надійних заходів захисту інформації на основі результатів дослідження може підвищити конкурентоспроможність організацій в Україні. Це може допомогти зміцнити довіру з клієнтами, партнерами та зацікавленими сторонами, демонструючи прихильність до захисту конфіденційної інформації.

Робота над цією темою має потенціал зробити внесок у наукові знання, спрямувати розробку політики безпеки та дати можливість організаціям в Україні покращити практику інформаційної безпеки, що зрештою призведе до покращеного захисту від несанкціонованого доступу.

Обґрунтування структури кваліфікаційної (дипломної) роботи

Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

Перший розділ охоплює основні поняття та значення захисту інформації, аналізує внутрішні та зовнішні загрози для інформаційних систем, а також розглядає різні моделі захисту інформації (модель Белла-ЛаПадули, модель Біби та модель RBAC). Також тут досліджуються організаційні заходи з захисту інформації, включаючи політики інформаційної безпеки, тренінги з підвищення обізнаності, оцінку та управління ризиками, моніторинг та аудит інформаційної безпеки.

У другому розділі проведено порівняльний аналіз практик інформаційної безпеки в центральному та західному офісах групи компаній «Фокстрот». Дослідження включає аналіз організаційної структури та ключових ролей в інформаційній безпеці, використання моделей захисту інформації, впровадження стандартів ISO, моніторинг та аналіз загроз, регулярні аудити, фізичну безпеку, автентифікацію користувачів, політики та процедури

класифікації інформації, тренінги та підвищення обізнаності, реагування на інциденти, передачу інформації зовнішнім особам, стратегії резервного копіювання та аварійного відновлення. Також включено результати інтерв'ю з працівниками департаменту інформаційних технологій та служби безпеки.

Третій розділ присвячений розробці та впровадженню нових практик захисту інформації в групі компаній Foxtrot. Було розроблено детальний план впровадження рішень Ivanti, що включає закупівлю обладнання, навчання персоналу та тестування систем. Особлива увага приділена аналізу ризиків та розробці стратегій управління ними, а також детальному плануванню та тестуванню всіх компонентів системи для забезпечення їхньої ефективності.

Робота охоплює широкий спектр питань захисту інформації, включаючи теоретичні основи, практичні аспекти аналізу та впровадження нових методик. Це робить її важливим внеском у розвиток інформаційної безпеки та аналітичної культури в українських організаціях.

РОЗДІЛ 1. «ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В КОНТЕКСТІ АНАЛІТИЧНОЇ КУЛЬТУРИ ОРГАНІЗАЦІЙ»

Інформаційні системи є важливою частиною діяльності організацій, що збільшує їх залежність від надійності та безпеки цих систем. Перший розділ наукової роботи "Теоретичні основи захисту інформації в контексті аналітичної культури організацій" охоплює ключові концепції інформаційної безпеки та її роль у сучасному контексті. Розглядаються різні моделі захисту інформації, аналізуються основні загрози для інформаційних систем та властивості ефективних систем захисту. Особлива увага приділяється впливу аналітичної культури організацій на захист інформації та огляду організаційних заходів для забезпечення інформаційної безпеки.

1.1. Поняття захисту інформації та його значення в сучасному організаційному контексті

У сучасну цифрову епоху інформаційна безпека стала критично важливим аспектом для організацій у різних галузях. Захист конфіденційних даних має першорядне значення для підтримки довіри зацікавлених сторін, забезпечення дотримання нормативних актів і захисту від потенційних загроз.

Інформаційна безпека відноситься до практики захисту інформації шляхом зменшення інформаційних ризиків. Це передбачає захист даних від несанкціонованого доступу, розкриття, зміни та знищення, гарантуючи, що інформація залишається конфіденційною, зберігає свою цілісність і доступна авторизованим користувачам у разі потреби. Відповідно до Міжнародної організації зі стандартизації (ISO), інформаційна безпека – це «збереження конфіденційності, цілісності та доступності інформації» (ISO/IEC 27000:2018). [1]

Згідно з Законом України "Про захист інформації в автоматизованих системах", захист інформації включає комплекс організаційно-технічних заходів

та правових норм, спрямованих на запобігання завданню шкоди інтересам власників інформації та користувачів автоматизованих систем. [6]

Відповідно до статті 1 Закону України "Про інформацію", захист інформації можна трактувати як сукупність правових, адміністративних, організаційних, технічних та інших заходів, спрямованих на забезпечення збереження, цілісності інформації та належного порядку доступу до неї. Це означає, що захист інформації передбачає комплексний підхід до забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів, що можуть належати як державним органам, так і приватним суб'єктам. [7]

Важливість інформаційної безпеки неможливо переоцінити в контексті сучасних організацій. Зі збільшенням залежності від цифрових інформаційних систем організації стикаються з численними ризиками, включаючи кібератаки, витоки даних і внутрішні загрози. Наслідки недотримання правил інформаційної безпеки можуть бути серйозними, включаючи фінансові втрати, репутаційні збитки, правові наслідки та збої в роботі. Ризики та загрози аналітичної культури перечислено у таблиці 1.1. (Додаток А)

Крім того, важливо визнати етичні та психологічні наслідки, які виникають для користувачів, працівників і власників інформації та інформаційних систем. Якщо говорити про порушення безпеки критично важливих програм, що використовуються в уряді чи військовій адміністрації, атомній енергетиці, медицині, аерокосмічній промисловості та фінансовому секторі, потенційні наслідки виходять далеко за межі індивідуального чи організаційного впливу. Насправді такі порушення можуть мати серйозні наслідки для навколишнього середовища, економіки, національної безпеки, здоров’я населення та навіть людських життів.

Захист особистих, фінансових даних і даних інтелектуальної власності має важливе значення для підтримки довіри клієнтів, партнерів і співробітників, а ефективні заходи безпеки інформації зменшують ризик збоїв, спричинених кіберінцидентами, забезпечуючи безперервність критично важливих бізнес-операцій.

Організації, відомі надійними методами захисту інформації, мають більше шансів завоювати довіру зацікавлених сторін, покращуючи свою репутацію та конкурентну перевагу.

1.2. Аналітична культура організацій

Концепція аналітичної культури в організаціях стала критично важливим фактором у використанні потужності даних для розробки стратегій і оцінювання ефективності роботи.

Аналітична культура відноситься до колективних практик, цінностей і поглядів в організації, які надають перевагу використанню даних і аналітичних методів для інформування про прийняття рішень і досягнення бізнес-результатів. Вона втілює в собі прагнення використовувати аналітичні дані для спрямування стратегічних ініціатив, підвищення операційної ефективності та сприяння інноваціям. Згідно з Давенпортом і Харрісом (2007), аналітична культура характеризується систематичним підходом до збору даних, аналізу та застосування на всіх рівнях організації. [16]

Значення аналітичної культури в сучасних організаціях полягає в її здатності перетворювати дані в практичні ідеї, тим самим покращуючи процеси прийняття рішень і сприяючи конкурентній перевазі. Організації з сильною аналітичною культурою можуть використовувати отримані дані для визначення тенденції та можливостей шляхом систематичного аналізу даних, оптимізації процесів, зменшення витрат та підвищення загальної ефективності.

Аналітична культура заохочує експерименти та інновації, надаючи фактичну основу для перевірки нових ідей і підходів, а також розуміння поведінки клієнтів за допомогою аналізу даних, що дозволяє адаптувати свої пропозиції, а також відіграє ключову роль у формуванні стратегій управління, забезпечуючи надійну основу для планування та виконання на основі даних. Основні аспекти включають планування на основі фактичних даних, вимірювання ефективності та аналіз можливих сценаріїв. [17]

Хорошим прикладом може стати Інститут аналітики та адвокації, який зосереджує свою роботу на розвитку громадянського суспільства, аналізі політик

і даних, а також створенні та впровадженні інноваційних цифрових рішень. Центр має на меті проведення досліджень та поширення їх результатів для допомоги органам влади в прийнятті ефективних рішень при форму-ванні та реалізації політик. [13]

Значний вплив вона має і на інформаційну безпеку, надаючи інструменти та мислення, необхідні для виявлення, оцінки та пом’якшення ризиків. Передові аналітичні методи, такі як виявлення аномалій і машинне навчання, можуть ідентифікувати потенційні загрози безпеці в режимі реального часу, дозволяючи організаціям вживати профілактичних заходів для запобігання порушенням, а використання оцінки ризиків на основі даних для оцінки ймовірності та впливу загроз безпеці, гарантує пріоритетність заходів безпеки на основі їх потенційного впливу. У разі інциденту безпеки аналітична культура забезпечує швидке й ефективне реагування за допомогою даних, щоб зрозуміти масштаб і характер порушення. Цей підхід підвищує ефективність і результативність зусиль реагування на інциденти.

Окрім посилення заходів безпеки, аналітична культура сприяє формуванню в організаціях культури безпеки, використовуючи отримані дані для виявлення прогалин у знаннях і адаптації програм навчання з безпеки відповідно до конкретних потреб. Цей цілеспрямований підхід покращує обізнаність працівників і дотримання правил безпеки. Безперервний моніторинг допомагає виявити та усунути вразливі місця, перш ніж ними можна буде скористатися. [23]

1.3. Загрози та властивості інформаційних систем

Інформаційні системи є невід’ємною частиною діяльності сучасних організацій, полегшуючи управління даними, спілкування та прийняття стратегічних рішень. Однак ці системи чутливі до широкого спектру загроз і вразливостей, які можуть поставити під загрозу їх цілісність, конфіденційність і доступність.

Експерт у сфері забезпечення комплексного управління ризиками підприємств та об'єктів критичної інфраструктури – Юрій Когут, у своїй книзі «Цифрова трансформація економіки та проблеми кібербезпеки» виділяє декілька типів різних внутрішніх та зовнішніх загроз. [27]

1.3.1. Інсайдерські загрози

Внутрішні загрози походять зсередини організації і можуть бути навмисними або ненавмисними. Їх часто складніше виявити та пом’якшити через довіру до колег. До основних внутрішніх загроз включають:

Зловмисні інсайдери, такі як незадоволені співробітники, можуть використовувати свій доступ до інформаційних систем для викрадення даних, збій операцій або сприяння зовнішнім атакам. Інсайдерські загрози є особливо небезпечними через те, що інсайдери добре знають систему та її вразливі місця.

Інсайдерами можуть бути середньостатистичні співробітники компанії: бухгалтер, менеджер з продажу, маркетолог, офіс-менеджер тощо, тобто будь-який працівник зі штату, який має доступ до певної корпоративної інформації. Інсайдери можуть володіти паролями, тобто законним доступом до комп’ютерних систем, якими вони оперують у своїй щоденній роботі. Співробітники також часто мають прямий доступ до конфіденційної інформації компанії. Це спрощує завдання обходити захисні бар’єри і робить цінні для компанії активи вразливими.

Доступ до внутрішньої інформації означає, що у співробітників немає необхідності незаконно проникати в мережу крізь зовнішній периметр, вони вже і так перебувають у системі. Загрозу також можуть становити програми, навмисно встановлені на комп’ютерах співробітниками, яких звільнили. Так, звільнені співробітники нерідко можуть представляти для компанії загрозу більш серйозну, ніж хакери. При тому, що це можуть бути як звільнені, так і працівники, які пішли за власним бажанням, у яких залишилися претензії до роботодавця або осад від минулих конфліктів. [11]

Фахівці з інформаційної безпеки констатують, що неуважність компаній до закриття облікових записів і обмеження доступу для колишніх співробітників – це справжня кіберзагроза, іноді навіть більш згубна, ніж втручання сторонніх осіб.

Агентство «Osterman Research» провело опитування в США і Канаді, яке показало, що 89% звільнених співробітників підприємств малого і середнього бізнесу зберігають доступ до корпоративних веб-додатків та електронної пошти. Кількість тих, хто вважає, що це дозволило б їм отримувати конфіденційну інформацію про роботу компанії – 45%. Стільки ж зізналося, що і після звільнення іноді користувалися своїм корпоративним обліковим записом, а 68% переносили робочі файли в приватне «хмарне» сховище за межами контролю корпоративної ITслужби, іноді для забезпечення конкурентної переваги в новій компанії.

Ці цифри – вагомий аргумент всерйоз задуматися власнику бізнесу про інформаційну безпеку та не ігнорувати заходи безпеки щодо колишніх працівників.

Щоб сформувати дієву систему захисту у аналітичних структурах структурах, необхідно класифікувати загрози, які надходять від інсайдерів.

Незаконне розголошення: в результаті незаконного розголошення, іншими словами, витоку, конфіденційні відомості залишають внутрішній периметр і потрапляють до рук осіб, які не мають прав на їх використання.

Наприклад, це можуть бути база даних клієнтів, інформація про контрагентів, інтелектуальна власність. Для здійснення подібних дій інсайдер має кілька найпоширеніших способів:

• відправка інформації через вихідні Інтернет-канали: наприклад, через електронну пошту;

• скачування даних на зовнішні накопичувачі;

• роздрукування конфіденційних документів на принтері.

У разі, коли інсайдери обізнані про те, що в компанії діють засоби фільтрації пошти, – вони можуть спробувати обійти це обмеження. Наприклад,

за допомогою перетворення даних (шифрування, трансформації в графічний вигляд, складної архівації) зловмисники можуть уникнути фіксації фільтрів.

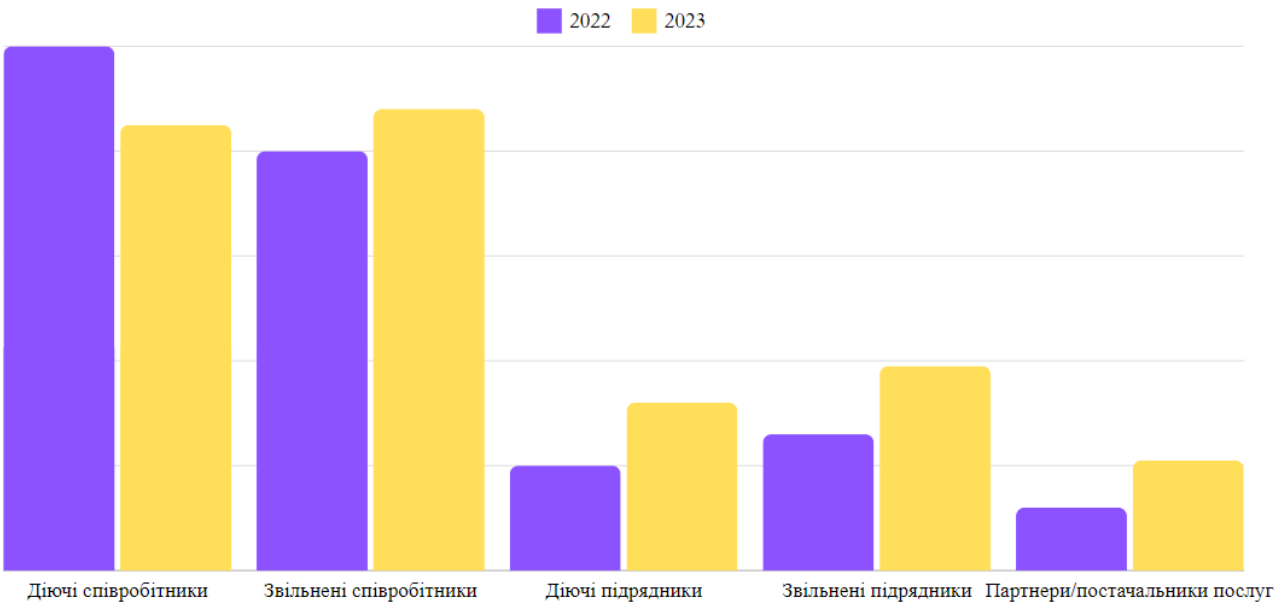
«Людський фактор»: дії співробітників, такі як випадкові видалення даних, неправильні конфігурація систем або попадання на фішингові атаки, які можуть призвести до серйозних порушень безпеки. Часто інсайдери піддають корпоративну інформацію ризику ненавмисно. Наприклад, можуть випадково завантажити корпоративні матеріали в Інтернет, записати дані на особистий комп'ютер, який потім вкрадуть, а також помилково відправити важливі документи третій стороні. Людська помилка залишається однією з головних причин інцидентів безпеки. [56]

Шахрайство і порушення авторських прав: одна з найрозповсюджених інсайдерських загроз – копіювання частини або крадіжка всього документу без зазначення авторства, таємне шифрування файлів, при якому компанія втрачає можливість працювати з ними, якщо пароль втрачено після звільнення недбалого співробітника. А найхрестоматійніша ситуація з погрозами всередині компанії – банальне шахрайство, з яким стикається кожна друга компанія. Найчастіше воно концентрується навколо махінацій з фінансовою документацією та обходу доступу до конфіденційної бази даних. [22]

Основним джерелом витоку інформації в Україні є Інтернет (33%). На переносні накопичувачі припало 19% усіх витоків інформації, на неелектронні носії – 12%5. Через корпоративний e-mail «втекло» 11% даних, 25% – втратили з інших причин.

У 2016 р. американська компанія «Spiceworks» провела дослідження проблем безпеки серед користувачів розробленої нею програми аудиту мережі. Аналіз ситуації дав несподіваний результат: основну загрозу безпеці становлять самі користувачі всередині підприємства. При чому ядро інсайдерської активності формується за рахунок елементарної необізнаності, низького порогу пильності внутрішніх користувачів і відсутності внутрішньої корпоративної культури захисту від загроз.

Те саме дослідження від компанії «Spiceworks» показало ще кілька цікавих цифр щодо диверсифікації джерел загроз для інформаційної безпеки:



- 36% – інсайдери;
- 25% – організовані угруповання зловмисників;
- 12% – терористичні угруповання;
- 12% – хакери.

При цьому найбільшу загрозу у витоку корпоративної інформації передусім несе людський фактор (рис. 1)

Рис.1 Соціотехнічний фактор у здійсненні витоку корпоративної інформації

Графік ілюструє соціотехнічні фактори, які сприяють витоку корпоративної інформації, за даними 2022 та 2023 років. Дані були отримані з наукової роботи Борсуковського Ю. В. та Бурячок В. Л. "Роль і місце вищих навчальних закладів у створенні системи інформаційної та кібернетичної безпеки України. Сучасний захист інформації". На графіку представлені наступні категорії: діючі співробітники, звільнені співробітники, діючі підрядники, звільнені підрядники, партнери/постачальники послуг. [39]

За аналізом графіка, можна зробити висновок, що соціотехнічні фактори витоків корпоративної інформації зазнали змін протягом 2022 та 2023 років.

Найбільш впливовими залишаються діючі співробітники, проте зросла значущість таких категорій, як звільнені співробітники, діючі підрядники та партнери/постачальники послуг. Це свідчить про необхідність посилення заходів безпеки не лише щодо діючих працівників, але й інших залучених сторін.

Такий стан справ вимагає динамічної адаптації корпоративної системи

інформаційної безпеки до поточних і постійно мінливих інформаційних загроз. Слід безперервно оцінювати ризики і ефективно управляти наявними фінансовими і технічними ресурсами відповідно до прийнятих політик корпоративної інформаційної безпеки, а також застосовувати ризик-орієнтований підхід до організації й забезпечення корпоративної безпеки, а це вимагає значних коштів (див. рис.2).

Рис.2 Інвестиції українських компаній в IT-безпеку (в середньому за рік)

Схема ілюструє обсяги фінансових вкладень українських компаній у корпоративну IT-безпеку в середньому за рік, розподілені за бізнесу: малий, середній та великий бізнес. З аналізу малюнка можна зробити висновок, що обсяги інвестицій у IT-безпеку зростають зі збільшенням розміру бізнесу. Великий бізнес інвестує значно більше як у загальному обсязі, так і в розрахунку на одного співробітника порівняно з малим та середнім бізнесом. Це свідчить про усвідомлення великими компаніями важливості IT-безпеки та відповідне виділення ресурсів для захисту інформації.

1.3.2. Зовнішні загрози

Зовнішні загрози створюються особами або організаціями за межами організації, часто зі злими намірами. Ці загрози різноманітні та постійно розвиваються завдяки прогресу технологій і зростаючій цінності цифрової інформації. Основні зовнішні загрози включають:

Кібератаки: кіберзлочинці використовують різноманітні методи, такі як зловмисне програмне забезпечення, програми-вимагачі та фішинг, щоб проникнути в інформаційні системи, викрасти дані або порушити роботу. Основними виконавцями кібератак є суб'єкти національної держави, хактивісти та організовані злочинні групи. [14]

Атаки на відмову в обслуговуванні (DoS): зловмисники переповнюють інформаційну систему надмірним трафіком, роблячи її недоступною для законних користувачів. Розподілені атаки типу «відмова в обслуговуванні» (DDoS), які включають кілька скомпрометованих систем, посилюють вплив.

Фізичні атаки: Несанкціонований фізичний доступ до інформаційних систем, чи то через крадіжку, вандалізм чи шпигунство, може поставити під загрозу безпеку та доступність даних.

Кібератаки росії на Україну є яскравим прикладом зовнішніх загроз інформаційній безпеці. З 2014 року Україна зіткнулася з серією складних кібератак, які приписують російським хакерам. Ці атаки спрямовані на критично важливу інфраструктуру, включаючи електромережі, державні та фінансові установи. До відомих інцидентів належать атаки 2015 та 2016 років на енергомережу України, які спричинили масові відключення електроенергії та підкреслили вразливість критичної інфраструктури до кіберзагроз. [26]

Після ескалації конфлікту у 2022 році частота та складність кібератак на Україну значно зросла. У день, коли росія почала вторгнення, кібератака була спрямована на Viasat, компанію супутникового зв'язку, яку використовують українські військові. Ця атака порушила зв'язок військових і різних секторів, продемонструвавши стратегічне використання кібератак у поєднанні з

кінетичними військовими операціями [28]. У квітні 2022 була виявлена кібератака, спрямована на енергетичну інфраструктуру України. Зловмисне програмне забезпечення під назвою Industroyer2 було розроблено для виведення з ладу електричних підстанцій і приписувалося тій самій групі, відповідальній за атаку на електромережі в 2016 році. Хоча атаку було зірвано, вона підкреслила триваючу загрозу для критичної інфраструктури України [38]. Деструктивне програмне забезпечення HermeticWiper, було застосовано проти різних українських організацій, стираючи дані та приводячи системи в непрацездатний стан. Ця атака збіглася з фізичним вторгненням, спрямованим на створення хаосу та перешкоджання комунікації та операційним можливостям [51] .Також, повідомлялося про безперервні фішингові кампанії, націлені на українських урядовців і військовослужбовців. Ці кампанії часто застосовують складні тактики соціальної інженерії, щоб скомпрометувати облікові дані та отримати доступ до конфіденційної інформації, впливаючи на прийняття рішень і операційну безпеку (CERTT).

Програмне забезпечення без виправлень і застарілі програми можуть містити вразливості, які зловмисники використовують, щоб отримати доступ або порушити роботу. Це включає вразливості в операційних системах, програмах і компонентах сторонніх розробників. Слабкі механізми автентифікації: слабкі паролі, відсутність багатофакторної автентифікації та неправильне керування обліковими даними користувача можуть призвести до неавторизованого доступу до інформаційних систем, а неадекватні заходи безпеки мережі, такі як неправильно налаштовані брандмауери, незашифровані канали зв’язку та незахищені служби, можуть наражати інформаційні системи на зовнішні загрози.

Стандартні конфігурації програмного та апаратного забезпечення часто включають непотрібні служби, відкриті порти та облікові дані за замовчуванням, якими можуть скористатися зловмисники. Нездатність зміцнити системи збільшує поверхню атаки.

Для усунення цих вразливостей потрібно реалізовувати багатофакторну автентифікації, застосовувати політики надійних паролів і використання біометричної автентифікації. Регулярні оновлення програмного забезпечення та систем за допомогою найновіших виправлень безпеки та оновлень має вирішальне значення для пом’якшення відомих вразливостей. Автоматизовані рішення для керування виправленнями можуть спростити цей процес, а розгортання брандмауерів, систем виявлення та запобігання вторгненням (IDPS) і віртуальних приватних мереж (VPN) може захистити від мережевих атак. Регулярні перевірки та сегментація мережі можуть додатково підвищити безпеку. [39]

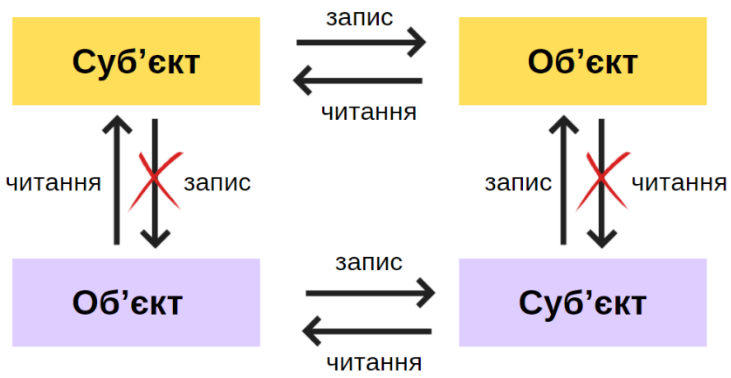
У відповідь на постійні кіберзагрози Україна вжила різноманітних заходів для посилення своєї інформаційної безпеки. Вони включають посилення кіберзахисту, покращення можливостей реагування на інциденти та сприяння міжнародній співпраці. Створення кіберполіції у 2015 році та партнерство з НАТО та Європейським Союзом відіграли ключову роль у розбудові стійкості України проти кібератак. [55]

1.4. Моделі захисту інформації

У інформаційній безпеці, що постійно змінюється, ефективні моделі захисту інформації є вирішальними для захисту конфіденційних даних і підтримки цілісності, конфіденційності та доступності інформаційних систем.

1.4.1. Модель Белла-ЛаПадули

Модель Белла-ЛаПадули (BLP), розроблена в 1970-х роках, є формальною моделлю безпеки, зосередженою на збереженні конфіденційності даних у військовому та урядовому контекстах. Сутність системи полягає в тому, що кожному суб'єкту (особі, яка взаємодіє з документами) та кожному об'єкту (документу) присвоюється рівень конфіденційності. Ці рівні варіюються від найвищого «Top Secret» (жовтий) до найнижчого «Unclassified» (фіолетовий). Важливим аспектом є те, що суб'єкт, який має доступ до документів з нижчим



рівнем конфіденційності, не може отримати доступ до документів з вищим рівнем конфіденційності. Крім того, суб'єкту забороняється здійснювати запис у документи з нижчим рівнем конфіденційності. Така система забезпечує суворий контроль за доступом та розповсюдженням інформації, запобігаючи можливості несанкціонованого доступу до конфіденційних даних та їх можливому компрометуванню (рис.3).

Рис.3 Модель Белла-ЛаПадули

1.4.2. Модель Biba

Модель Biba, представлена в 1977 році, розроблена для підтримки цілісності даних, а не конфіденційності, що передбачає:

1. Попередження модифікації даних неавторизованими сторонами.
2. Попередження неавторизованої модифікації даних авторизованими сторонами.
3. Підтримання внутрішньої та зовнішньої узгодженості даних (відповідності реальному світу).

Ця модель політики безпеки характеризується принципами: "Немає читання знизу, немає запису вгору" на противагу моделі Белла-ЛаПадули, яка описується як "Немає читання зверху, немає запису вниз".

Розглянемо цю концепцію на прикладі звичайної організації. В моделі Біби, працівники можуть створювати документи на своєму рівні або на нижчому рівні цілісності, але не можуть редагувати документи з вищим рівнем цілісності.

Наприклад, менеджер середньої ланки може створювати звіти для відділу, які можуть читати працівники цього відділу, але ці звіти не можуть бути змінені керівником вищої ланки. Навпаки, менеджер середньої ланки може переглядати стратегії і звіти, підготовлені керівником вищої ланки, але не може переглядати чернетки або внутрішні замітки, написані співробітниками з нижчим рівнем доступу.

Інша аналогія - система комунікації в корпоративному середовищі. Керівник відділу може надіслати завдання своїм підлеглим, і ці підлеглі можуть створювати відповідні документи або звіти, які можуть переглядати інші працівники відділу. Однак, ці документи не можуть бути змінені працівниками вищих рівнів управління. У такій системі, керівник завжди має доступ до документів, створених підлеглими, але не може переглядати або редагувати документи, створені на рівнях, нижчих за їхній власний.

Ця політика забезпечує, що кожен рівень організації має чітко визначені межі доступу і можливості редагування, що запобігає несанкціонованим змінам і зберігає цілісність важливої інформації.

1.4.3. Модель RBAC

Модель управління доступом на основі ролей (Role-Based Access Control, RBAC) є підходом до управління доступом до інформаційних ресурсів, який визначає права доступу користувачів на основі їхніх ролей у організації. У цій моделі ролі створюються відповідно до посадових обов'язків і функцій, які виконують співробітники. Ролі, у свою чергу, містять набір дозволів, які визначають дії, що можуть виконуватися над ресурсами, такими як файли, бази даних або програми.

Кожному користувачу призначається одна або кілька ролей, що спрощує управління доступом. Це дозволяє адмініструвати права доступу через ролі, а не через індивідуальні налаштування для кожного користувача. Такий підхід значно знижує складність управління доступом, особливо у великих організаціях. Дозволи, що входять до ролей, визначають конкретні дії, які можуть виконуватися над ресурсами, наприклад, читання, запис або видалення.

Таким чином, ролі об'єднують дозволи, щоб забезпечити потрібний доступ користувачам.

Основні переваги RBAC включають простоту управління, підвищену безпеку та гнучкість. Управління правами доступу здійснюється через ролі, що спрощує процес адміністрування, особливо в великих організаціях. Ролі можуть бути налаштовані таким чином, щоб забезпечити принцип найменших привілеїв, тобто користувачі отримують лише ті права доступу, які їм необхідні для виконання своїх завдань. Система також легко адаптується до змін у організаційній структурі, оскільки зміна ролі користувача автоматично змінює його дозволи.

У компанії може бути кілька ролей, таких як "Адміністратор", "Менеджер" та "Спеціаліст з підтримки". Кожна з цих ролей має певні дозволи. Наприклад, роль "Адміністратор" може мати доступ до всіх систем, можливість управління користувачами та налаштуваннями системи. "Менеджер" може мати доступ до звітів та аналітики, а також управління командою. "Спеціаліст з підтримки" може мати доступ до системи підтримки клієнтів і можливість оновлювати записи клієнтів.

Використання RBAC дозволяє ефективно керувати правами доступу співробітників, забезпечуючи високий рівень захисту інформаційних активів. Ця модель допомагає оптимізувати процеси управління доступом, мінімізувати ризики несанкціонованого доступу та підтримувати відповідність політикам безпеки компанії.

1.4.4. Вітчизняні моделі захисту інформації

Україна запровадила кілька правил і стандартів для забезпечення захисту інформації в межах своїх кордонів. Основою є Закон України «Про захист інформації», який встановлює правові основи захисту інформації як у державному, так і в приватному секторах. Ключові компоненти включають нагляд за впровадженням національної політики кібербезпеки та координацію між різними урядовими установами.

Державна служба спеціального зв’язку та захисту інформації (ДСЗЗІ) відповідає за розробку та впровадження стандартів (ДСТУ) та протоколів інформаційної безпеки, які подібні до стандартів ISO/IEC та містять рекомендації щодо управління інформаційною безпекою, оцінки ризиків та реагування на інциденти. [24]

Українські організації застосовують комбінацію передового міжнародного досвіду та місцевих нормативних актів для захисту своїх інформаційних систем. До них належать багаторівневі рамки безпеки інтеграції моделей BLP і Biba для досягнення балансу між вимогами конфіденційності та цілісності та використання оцінок ризиків для виявлення та пом’якшення потенційних загроз відповідно до стандартів ДСТУ.

Сучасні підходи до захисту інформації в організаціях включають архітектуру нульової довіри, поведінкову аналітику та використання штучного інтелекту і машинного навчання.

Архітектура нульової довіри — це підхід, при якому не довіряють нікому за замовчуванням, незалежно від того, де знаходиться користувач, пристрій чи мережа. Всі повинні постійно проходити перевірку, яка включає автентифікацію і авторизацію на основі даних про користувача, його місцезнаходження та стан пристрою. Користувачам надається доступ лише до мінімально необхідних ресурсів, відповідно до їхніх ролей та обов'язків. Системи створюються з припущенням, що порушення можливі, тому реалізується сегментація та шифрування, щоб мінімізувати вплив. Цей підхід особливо ефективний для захисту від складних кіберзагроз і для безпеки розподілених середовищ, таких як віддалена робота та хмарні сервіси.

Поведінкова аналітика полягає у моніторингу та аналізі поведінки користувачів для виявлення аномалій, які можуть бути загрозами. Це включає аналіз поведінки користувачів і суб’єктів за допомогою машинного навчання для визначення нормальної поведінки та виявлення відхилень, які можуть сигналізувати про внутрішні загрози або скомпрометовані облікові записи. Також важливим є моніторинг у реальному часі, який дозволяє безперервно

відстежувати дії користувачів і системні події для надання миттєвих сповіщень і відповідей на підозрілу поведінку. Поєднання даних про поведінку з контекстуальною інформацією, такою як шаблони доступу та історії транзакцій, підвищує точність виявлення загроз. Це дозволяє забезпечити проактивний і адаптивний захист від нових загроз.

Штучний інтелект (AI) та машинне навчання (ML) значно покращують захист інформації за рахунок автоматизації виявлення загроз, реагування на них та їх запобігання. Вони дозволяють виявляти аномалії та незвичайні шаблони поведінки, що можуть вказувати на інциденти безпеки, такі як вторгнення в мережу або викрадання даних. Прогнозна аналітика на основі історичних даних дозволяє передбачати майбутні загрози і вразливості, що дає змогу вживати попереджувальних заходів. Рішення на основі ШІ можуть автоматично реагувати на інциденти, стримуючи та пом'якшуючи загрози, що скорочує час реагування та мінімізує збитки. AI та ML забезпечують ефективність захисту інформації, надаючи інтелектуальні, адаптивні та масштабовані рішення безпеки.

Останніми роками українські організації все частіше використовують сучасні підходи до захисту інформації для боротьби зі складними кіберзагрозами та захисту своїх критично важливих даних. Серед цих організацій - Фокстрот, відома українська роздрібна мережа, що спеціалізується на електроніці та побутовій техніці, виділяється активним впровадженням передових заходів безпеки. Завдяки інтеграції архітектури нульової довіри, поведінкової аналітики та рішень на основі штучного інтелекту Фокстрот значно покращив рівень інформаційної безпеки, забезпечивши надійний захист від внутрішніх і зовнішніх загроз. [10]

Фокстрот прийняв архітектуру нульової довіри для посилення своєї системи безпеки, прийнявши принцип «ніколи не довіряй, завжди перевіряй». Цей підхід гарантує, що кожен запит на доступ, будь то всередині чи поза мережею, проходить ретельну автентифікацію та авторизацію на основі ідентифікації користувача, справності пристрою та інших контекстних факторів. Впровадивши багатофакторну аутентифікацію, сегментацію мережі та постійний

моніторинг, Фокстрот мінімізував ризик несанкціонованого доступу та витоку даних, створивши більш безпечне середовище для своєї діяльності.

Фокстрот використовує аналітику поведінки, щоб завчасно виявляти потенційні інциденти безпеки та реагувати на них. Застосовуючи аналітику поведінки користувачів і суб'єктів (UEBA), організація може відстежувати дії користувачів і виявляти аномалії, які можуть вказувати на зловмисну поведінку або скомпрометовані облікові записи. Цей аналіз у реальному часі дозволяє Фокстроту швидко реагувати на загрози, зменшуючи ймовірність втрати даних або збоїв у роботі. Інтеграція контекстної обізнаності ще більше підвищує точність виявлення загроз, дозволяючи групі безпеки ефективніше розрізняти законні та підозрілі дії. Автоматизація процесів реагування на інциденти гарантує, що загрози локалізуються та нейтралізуються швидко, мінімізуючи вплив на бізнес-операції. [53]

Інші українські організації так само перейняли ці сучасні підходи до захисту інформації. Наприклад, Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ) запровадила принципи «нульової довіри» та виявлення загроз на основі штучного інтелекту для захисту урядових комунікацій і даних. Українські банки та фінансові установи, зокрема АТ «Сенс Банк», АТ "КРЕДІ АГРІКОЛЬ БАНК", Monobank та ін. також використовують поведінкову аналітику та машинне навчання для захисту від шахрайства та кібератак, забезпечуючи цілісність та конфіденційність інформації про клієнтів. [19]

Ці приклади демонструють ефективність сучасних моделей захисту інформації для підвищення рівня безпеки українських організацій. Застосовуючи інноваційні підходи, ці організації мають змогу краще орієнтуватися в складному ландшафті загроз, що розвивається, забезпечуючи захист своїх важливих даних і підтримуючи операційну стійкість.

1.5. Організаційні заходи з захисту інформації

Для захисту даних від несанкціонованого доступу, зломів та інших кіберзагроз необхідні ефективні заходи інформаційної безпеки. Політики інформаційної безпеки є основою системи безпеки організації. Вони забезпечують структурований підхід до управління та захисту інформаційних активів, визначають ролі та обов'язки співробітників і встановлюють інструкції щодо прийнятного використання.

Розробка політики інформаційної безпеки передбачає кілька ключових кроків:

1. Оцінка організаційних потреб.

2. Залучення зацікавлених сторін.

3. Відповідність нормативним вимогам.

4. Чітка та стисла документація.

Ефективне впровадження політики інформаційної безпеки вимагає поширення політики в організації через різні канали, встановлення процедур моніторингу відповідності та усунення порушень, а також навчання співробітників політикам і їхнім ролям у їх застосуванні.

Людська помилка є суттєвим фактором багатьох порушень безпеки. Тому освіта працівників з інформаційної безпеки має вирішальне значення. Програми підвищення обізнаності допомагають співробітникам зрозуміти потенційні загрози та важливість дотримання протоколів безпеки.

Для ефективного навчання інформаційній безпеці необхідно періодично проводити навчання (яке може включати імітацію фішингових атак) та адаптувати навчальні матеріалів до конкретних ролей і обов'язків співробітників. Важливо також проводити опитування для збору відгуків від співробітників про тренінги. Моніторинг звітів про інциденти дозволяє аналізувати частоту та характер інцидентів безпеки до та після навчальних ініціатив. Крім того, постійне вдосконалення змісту навчання на основі отриманих відгуків і аналізу інцидентів є важливою складовою процесу.

Оцінка та управління ризиками в контексті інформаційної безпеки включає декілька ключових етапів. Цей процес включає ідентифікацію активів,

що передбачає складання переліку всіх інформаційних активів та визначення їх важливості для організації. Аналіз загроз включає визначення потенційних загроз та їх джерел, а оцінка вразливості — оцінку слабких місць в існуючих заходах безпеки. Останнім етапом є аналіз впливу, що включає оцінку потенційного впливу різних загроз на організацію.

Управління ризиками включає декілька підходів. Зменшення ризиків передбачає впровадження заходів для зменшення ймовірності та впливу виявлених ризиків. Передача ризиків може здійснюватися за допомогою страхування або аутсорсингу для управління певними ризиками. Прийняття ризику означає визнання та прийняття ризику, коли пом’якшення неможливе. Постійний моніторинг включає регулярний перегляд та оновлення стратегій управління ризиками.

Розробка та впровадження систем моніторингу та аудиту інформаційної безпеки є важливим аспектом захисту даних. Вони необхідні для виявлення інцидентів безпеки та швидкого реагування на них.

Основними компонентами цих систем є:

1. Системи виявлення вторгнень (IDS), які моніторять мережевий трафік для виявлення підозрілих дій.

2. Системи безпеки та керування подіями (SIEM), що збирають та аналізують дані з різних джерел для виявлення потенційних загроз.

3. Сповіщення в режимі реального часу, що надають миттєві повідомлення про інциденти безпеки.

Системи аудиту допомагають забезпечити відповідність політикам безпеки та виявити сфери, які потребують вдосконалення.

Ефективні системи аудиту включають:

1. Регулярні аудити, які проводяться періодично для перевірки практик безпеки.

2. Комплексне звітування, що документує результати та надає практичні рекомендації.

3. Подальші аудити, що гарантують вирішення виявлених проблем та внесення покращень.

Планування реагування на інциденти інформаційної безпеки є вирішальним для мінімізації впливу порушень безпеки. Це включає розробку плану реагування на інциденти, що окреслює процедури для виявлення, реагування та відновлення після інцидентів. Важливо також створити групу реагування на інциденти, яка складається з навчених професіоналів, і чітко визначити ролі та обов'язки всередині цієї групи.

Ефективне управління інцидентами включає швидке виявлення та аналіз інцидентів безпеки, стримування загрози та усунення її джерела, а також відновлення нормальної роботи уражених систем і даних.

Діяльність після інциденту спрямована на покращення майбутнього реагування. Це включає аналіз першопричини інциденту, документацію всіх дій, вжитих під час реагування, аналіз інциденту та реагування для визначення областей для покращення, а також оновлення політик і процедур безпеки на основі отриманої інформації.

Висновки до розділу 1: у цьому розділі розглянуто захист інформації в сучасних організаціях, який є надзвичайно важливим для забезпечення конфіденційності, цілісності та доступності даних. В умовах зростаючої залежності від цифрових технологій, організації повинні впроваджувати комплексні заходи безпеки, що є критично важливим для підтримки довіри зацікавлених сторін, дотримання нормативних актів та захисту від потенційних загроз.

Аналітична культура організацій сприяє прийняттю рішень на основі даних, оптимізації процесів та підвищенню ефективності роботи. Вона дозволяє виявляти потенційні загрози безпеці та вживати відповідних заходів для їх запобігання, формуючи культуру безпеки всередині організацій і підвищуючи обізнаність працівників про важливість захисту інформації.

Інформаційні системи піддаються як внутрішнім, так і зовнішнім загрозам. Для ефективного захисту необхідно класифікувати загрози та впроваджувати відповідні заходи безпеки, такі як багатофакторна автентифікація та регулярні оновлення програмного забезпечення. Моделі захисту інформації, такі як моделі Белла-ЛаПадули, Біба та *RBAC*, забезпечують різні аспекти захисту даних, підтримуючи конфіденційність, цілісність та доступність інформації.

Політики інформаційної безпеки є основою для захисту даних в організаціях. Вони включають розробку, впровадження та моніторинг політик безпеки, навчання працівників, оцінку ризиків та управління інцидентами. Регулярні аудити та системи моніторингу допомагають виявляти та швидко реагувати на загрози, забезпечуючи мінімізацію наслідків порушень безпеки та покращення майбутніх заходів.

РОЗДІЛ 2. «АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОФІСАХ ГРУПИ КОМПАНІЙ «ФОКСТРОТ»: РЕГІОНАЛЬНИЙ АСПЕКТ»

Другий розділ наукової роботи присвячений аналізу інформаційної безпеки в регіональних офісах групи компаній «Фокстрот», зокрема в центральному офісі у Києві та західному офісі у Львові. Огляд включає оцінку існуючих систем захисту даних, політик доступу, процедур автентифікації та авторизації, а також обізнаності співробітників щодо загроз інформаційній безпеці. Використовуючи методи інтерв'ювання, аналізу документів та спостереження, буде визначено слабкі місця у системах захисту і враховано регіональні особливості функціонування офісів. Також розглянуто вплив технічної інфраструктури, підготовки персоналу та регіональних кіберзагроз на рівень інформаційної безпеки.

2.1. Загальна характеристика групи компаній Foxtrot

Група компаній «ФОКСТРОТ» є однією з найбільших комерційних структур України, яка стабільно функціонує в економічному просторі країни та активно сприяє розвитку громадянського суспільства. Заснована у 1994 році, компанія розпочала свою діяльність з оптового продажу побутової техніки та електроніки. Завдяки наполегливій праці засновників, вже з 1996 року компанія почала розвивати роздрібну торгівлю, відкривши перший магазин у Харкові. У 1997 році, з відкриттям супермаркету на вул. Дегтярівській у Києві, "Фокстрот" офіційно став роздрібним торговцем, що заклало основу для подальшого розвитку мережі. [57]

У 2008 році було проведено реформування менеджменту Групи компаній «ФОКСТРОТ» з метою підвищення ефективності інвестицій у бізнес- проєкти та надання їм якісних сервісних послуг. Це дозволило компанії значно покращити управління та розширити свої можливості на ринку.

До складу ГК «ФОКСТРОТ» входять такі бренди, як "Фокстрот. Техніка для дому", "Техношара" (ритейл побутової та електронної техніки), а також «DEPO't Center» і «Fantasy Town» (управління нерухомістю). Кожен з цих брендів має свою унікальну історію та значний внесок у розвиток Групи компаній. Бренди від Групи компаній «ФОКСТРОТ» представлені розгалуженими по всій Україні мережами сучасних магазинів і центрів сервісного обслуговування, де працює понад 10 тисяч осіб. Оптимальна система управління, потужний інвестиційний ресурс, ефективна координація та кооперація дій, проведення спільних маркетингових заходів забезпечують високий авторитет брендів ГКФ і стабільний розвиток підприємств, які розвиваються під цими брендами. Це сприяє довірі найвідоміших міжнародних компаній, міцним партнерським відносинам з діловими колами у всіх регіонах України і заслуженому суспільному визнанню брендів.

З 2012 року "Фокстрот" активно впроваджує цифрові трансформації, переходячи на омніканальну бізнес-модель, яка інтегрує онлайн і офлайн канали продажів. Цей крок дозволив компанії адаптуватися до сучасних вимог ринку та забезпечити зручність покупок для клієнтів. Перші підсумки діджиталізації були зафіксовані у 2015 році, а у 2018 році торгівельна мережа "Фокстрот" стала єдиним організмом зі спільними акціями, сервісами та програмою лояльності. У 2019 році компанія провела масштабний ребрендинг під гаслом «Оновлюйся!», що включав зміну позиціювання, візуального стилю, tone of voice та оновлення магазинів.

Станом на 2023 рік, "Фокстрот" є однією з найбільших роздрібних мереж електроніки та побутової техніки в Україні за кількістю магазинів і обсягами продажів. Мережа налічує 120 магазинів у 67 обласних і районних центрах, з яких три працюють як точки видачі інтернет-замовлень. Онлайн-магазин foxtrot.ua щомісяця відвідують майже 3,2 мільйони користувачів, а програма лояльності «ФоксFan» об'єднує понад 13,5 мільйонів учасників.

"Фокстрот" першим серед ритейлерів електроніки запровадив програмне РРО (касу в смартфоні), інтегрував цифрові чеки у мобільні банкінги, а також

надав можливість оплати криптовалютою. Ритейлер поступово інтегрує найсучасніші способи оплати товарів, такі як через чат-боти у Viber і Telegram, VisaQR, LiqPAY, Apple Pay та Google Pay.

У 2009 році компанія DEPOT Development Group вивела на ринок бренд DEPO’t Center™, представлений мережею торговельно-розважальних центрів у регіонах України з чисельністю населення понад 50 тисяч осіб. Сьогодні центри DEPO't Center™ щодня приймають 10-15 тисяч відвідувачів у Чернівцях, Лубнах, Миколаєві, Кропивницькому та Черкасах. Бренд DEPO’t Center™ об'єднує торговельно-розважальні, торговельно-офісні та торгові центри, надаючи великий вибір різних товарів, послуг та розважальних проєктів. Маркетингова стратегія спрямована на розвиток культури шопінгу та відпочинку для всієї родини.

DEPO’t Center™ не тільки комерційний, а й соціальний проєкт. Однією з головних складових центру є розважальна частина - Fantasy Town™, що орієнтована на сімейний та колективний відпочинок. Depo't center™ бере активну участь у соціальному розвитку регіонів, організовуючи та підтримуючи молодіжні ініціативи.

"Фокстрот" є учасником спільноти «Бізнес без бар’єрів», дотримуючись принципів безбар’єрного ведення бізнесу і став першим у галузі, хто виступив ініціатором адаптації мережі до потреб нечуючих відвідувачів.

Група компаній «ФОКСТРОТ» також активно підтримує соціальні та екологічні ініціативи, такі як «Зелений офіс», «ЕКОкласс» та «Школа безпеки», що розвивається за участю ДСНС України. Компанія дотримується принципів Глобального Договору ООН про соціальну відповідальність бізнесу.

У квітні 2023 року Група компаній «ФОКСТРОТ» отримала нагороду «Сміливий бізнес, що змінює країну» від експертної організації Центр «Розвиток КСВ» за корпоративний кейс «Рік війни. Партнерство заради незалежності України та зміцнення бізнесу». Ця нагорода визнає синергію з державними та комерційними партнерами, яка стала інструментом боротьби за незалежність України та виживання бізнесу.

Керівниками Групи компаній «ФОКСТРОТ» є Валерій Маковецький і Геннадій Виходцев, а керівником мережі "Фокстрот" – Олексій Зозуля. Завдяки їхній наполегливій праці та стратегічному баченню, компанія продовжує впроваджувати інновації та підтримувати високі стандарти бізнесу в Україні, демонструючи стійкість і адаптивність у складних умовах.

Група компаній «ФОКСТРОТ» є однією з найбільших комерційних структур України і складається з багатьох відділів, у тому числі відділ інформаційної безпеки, до якого також входять відділи підтримки IT-інфраструктури та підтримки користувачів (рис. 4).

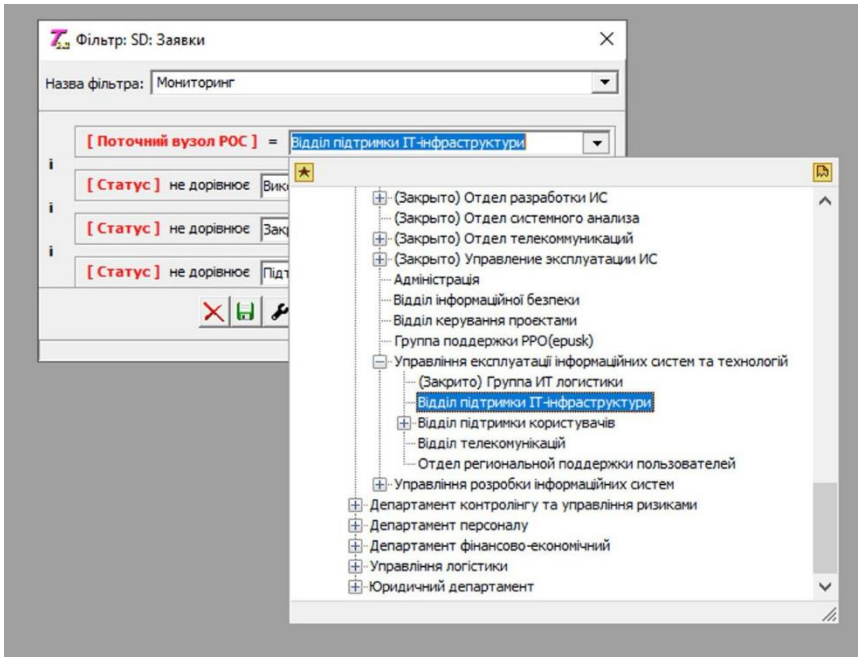


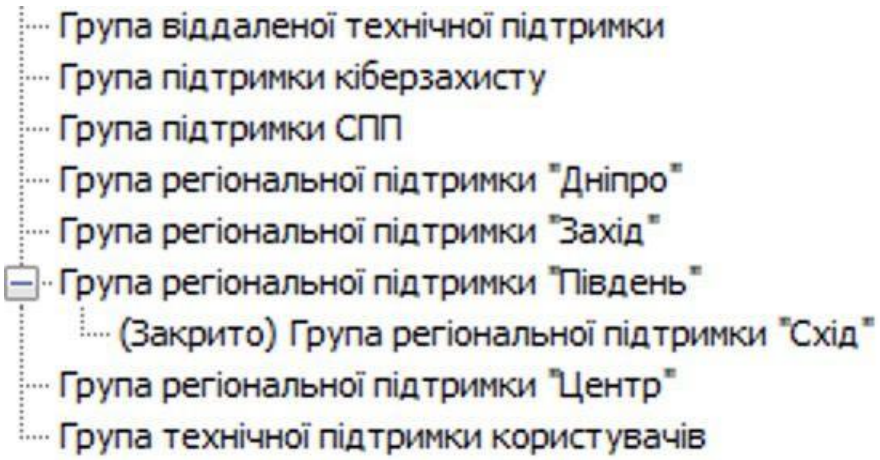
Рис.4 Інтерфейс спец. ПЗ «Typhoon» з ієрархією відділу інформаційної безпеки ГК «Фокстрот»

Відділ IT інфраструктури відіграє ключову роль у забезпеченні безпеки аналітичних даних. Його задачі включають впровадження та адміністрування систем захисту даних від несанкціонованого доступу, використання засобів шифрування як у стані спокою, так і при передачі, а також створення і підтримку політик доступу, що контролюють, хто і яким чином має доступ до аналітичних даних. Важливим аспектом є виявлення та реагування на інциденти безпеки через налаштування і моніторинг систем виявлення та запобігання вторгнень, відстеження підозрілої активності в мережі та на серверах, розробку і

впровадження планів реагування на інциденти, які включають аналіз та мінімізацію їх наслідків.

До обов’язків працівників відділу підтримки входить проведення тренінгів з питань інформаційної безпеки для працівників компанії впровадження та програми безперервного навчання з акцентом на новітні методи та засоби захисту даних. Управління інцидентами та відновлення після аварій включають розробку та тестування планів відновлення після збоїв та катастроф, забезпечення регулярного резервного копіювання даних та перевірку можливості відновлення з цих копій, а також відновлення аналітичних даних та систем у разі інцидентів безпеки або інших аварійних ситуацій.

Група компаній "Фокстрот" має розгалужену структуру, яка включає п’ять регіональних відділів: група регіональної підтримки "Центр", "Дніпро", "Захід", "Південь" та "Схід". Кожен з цих відділів відповідає за надання підтримки та управління операціями у відповідних регіонах України. Однак через повномасштабне вторгнення відділ "Схід" у Донецькій області наразі не функціонує, а підтримкою користувачів з цього відділу займається група



«Південь» (рис. 5).

Рис.5 Інтерфейс спец. ПЗ «Typhoon» з ієрархією груп підтримки користувачів

У науковій роботі будуть детально розглянуті два офіси групи компаній "Фокстрот" – "Центр" (м. Київ) та "Захід" (м. Львів). Дослідження зосередиться на аналізі політики інформаційної аналітичної безпеки цих офісів, оцінці

ефективності впроваджених заходів захисту даних, а також порівнянні їх підходів до управління безпекою. Такий підхід дозволить виявити регіональні особливості та кращі практики, які можуть бути застосовані для покращення загального рівня безпеки в компанії.

2.2. Порівняльний аналіз Західного та Центрального офісів

Центральний офіс ГК "Фокстрот" розташований у Києві, столиці України, що є найбільшим містом та основним діловим центром країни. Це забезпечує легкий доступ до ключових партнерів, постачальників та регуляторів, а також великий ринок праці.

Маючи розвинену інфраструктуру, київський офіс включає сучасні офісні приміщення, потужний IT-відділ та великий логістичний центр. Після знищення складу в Гостомелі під час вторгнення рф у 2022 році, компанія відкрила новий склад у с. Колонщина, Київської області, площею 22 тисячі кв. м. В цьому офісі працює значний штат співробітників, зосереджуючи на собі керівні, стратегічні та адміністративні функції. Понад 10 тисяч осіб працюють у мережі компанії по всій Україні, з яких значна частина зосереджена саме тут.

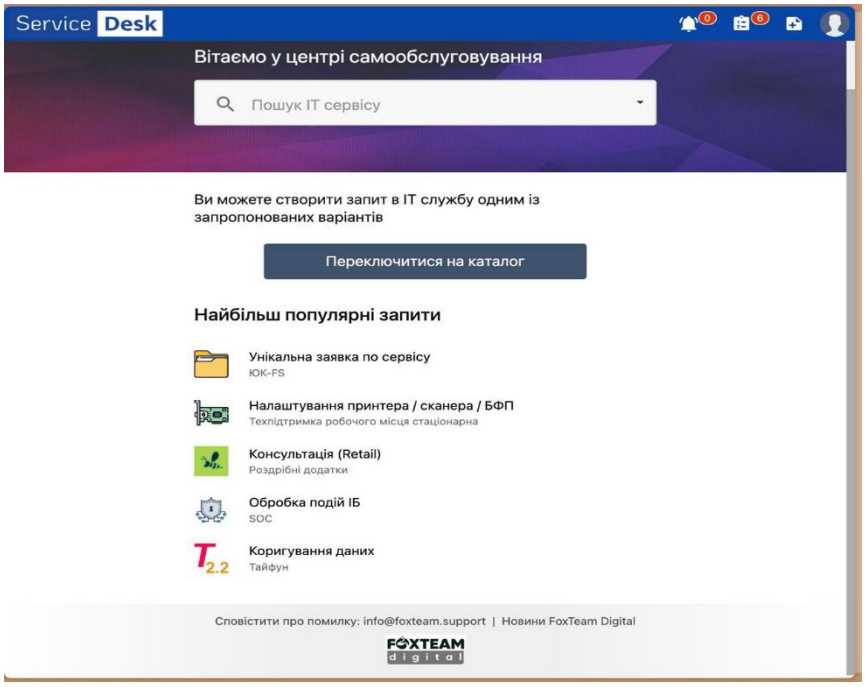
Київський офіс займається розробкою стратегій розвитку, управлінням фінансами, маркетингом, HR, юридичними питаннями, а також підтримує та координує роботу регіональних офісів і магазинів. Тут приймаються ключові рішення щодо інвестицій, розширення мережі та впровадження нових технологій. Розташування в Києві дозволяє швидко реагувати на зміни в законодавстві, регуляторних вимогах та ринкових умовах, що сприяє ефективному управлінню компанією та підтримці конкурентних переваг.

Вся інформаційна безпека групи компаній централізовано управляється з Києва. Впроваджуються сучасні заходи з інформаційної безпеки, включаючи багатофакторну автентифікацію, регулярні оновлення програмного забезпечення та використання сучасних антивірусних систем. Особлива увага приділяється захисту конфіденційних даних клієнтів та комерційної інформації. Центральний офіс обслуговує сервер D1, який містить 70% серверів компанії, та орендує

сервер parkovy_Kyiv. Також центральний офіс = у своєму підпорядкуванні має сервер A2, проте інформація про його місце розташування є конфіденційною.

Західний офіс ГК "Фокстрот" розташований у Львові, культурному та економічному центрі Західної України. Львів забезпечує стратегічний доступ до ринків Західної України та Європейського Союзу. Офіс обладнаний сучасними офісними приміщеннями та має доступ до потужних IT-ресурсів. Під час війни компанія тимчасово релокувала частину своїх операційних функцій у Львів, що дозволило забезпечити безперервність бізнесу.

Підтримка користувачів у Західному офісі організована за трьома лініями. Перша лінія займається прийомом заявок, друга – прийомом заявок і їх усуненням, третя лінія зосереджена на серверній інфраструктурі. Заявки можуть включати різні технічні проблеми, питання користувачів та запити на підтримку. Користувач, стикаючись з проблемою або маючи запит, може створити заявку через Service Desk (рис.8,9) або надіслати електронний лист до служби підтримки. Після входу, користувач заповнює відповідну форму заявки, вказуючи тип проблеми або запиту, описуючи деталі ситуації, додаючи скріншоти або інші необхідні файли для кращого розуміння проблеми. Заповнивши всі необхідні поля, користувач надсилає заявку, яка проходить обробку першою лінією підтримки, та за необхідності передається на другу лінію



підтримки (рис.10).

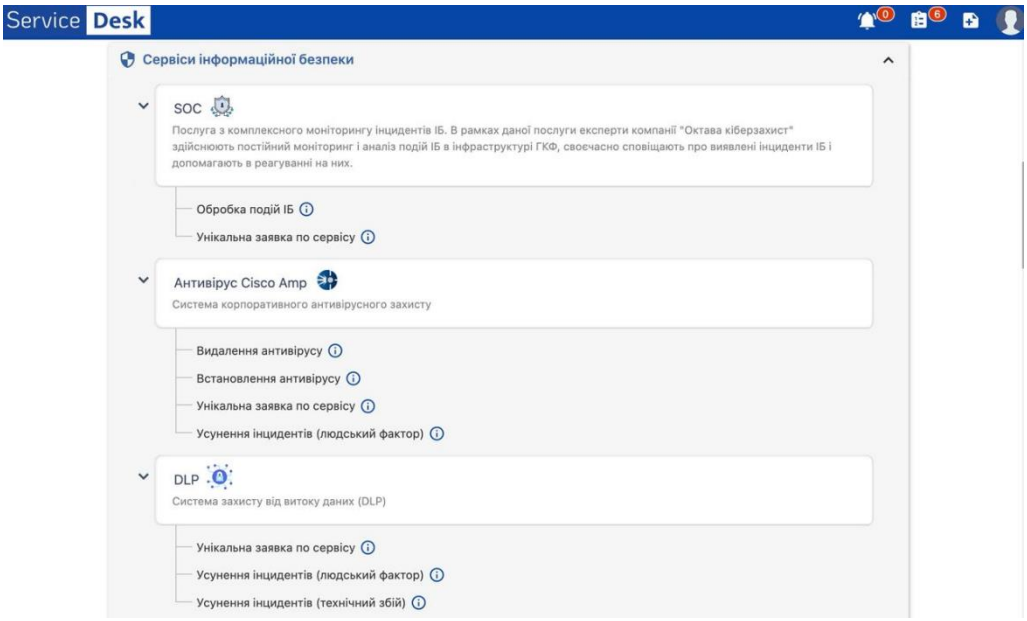
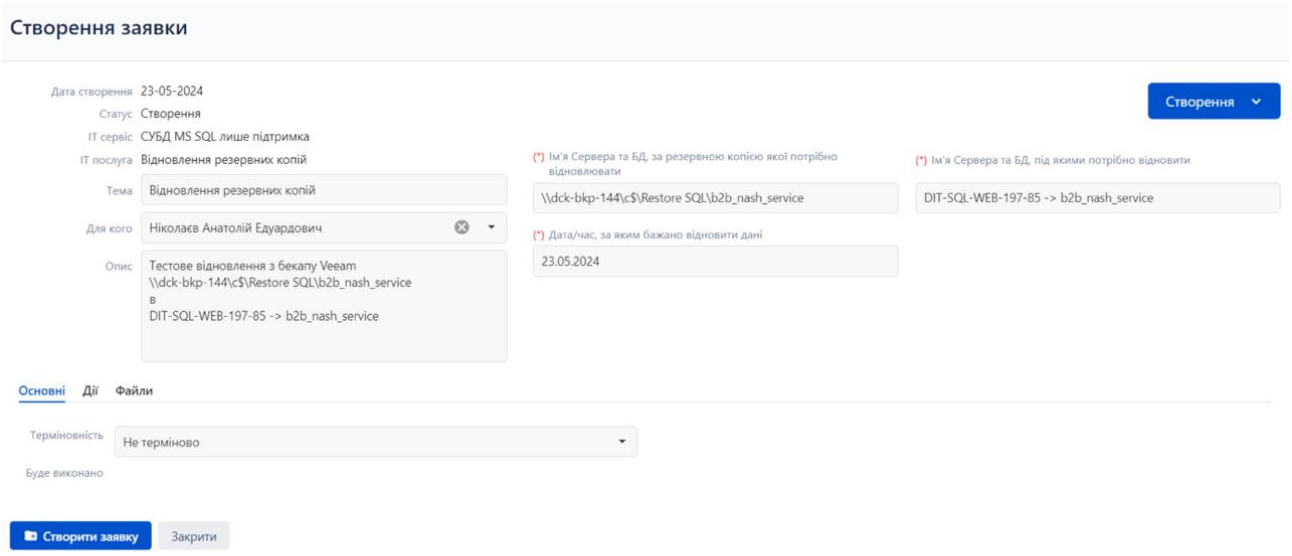


Рис.8 Інтерфейс спец. ПЗ «ServisDesk» у IT-відділі FoxTeam

Рис.9 Інтерфейс спец. ПЗ «ServisDesk» у IT-відділі FoxTeam



(приклади сервісів інформаційної безпеки)

Рис.10 Приклад заповненої користувачем заявки,
яка передається на другу лінію підтримки

Виділяються такі типи заявок:

- Технічні проблеми (збої в роботі програмного забезпечення, проблеми з доступом до сервісів)
- Питання користувачів (консультації щодо використання програмного забезпечення, налаштування обладнання)

- Запити на підтримку (оновлення програмного забезпечення, встановлення нових додатків)

Заявки, пов’язані з аналітичною безпекою, можуть включати:

- Моніторинг і аналіз загроз (запити на перевірку підозрілої активності в системі, аналіз потенційних вразливостей)
- Оновлення систем безпеки (запити на впровадження нових методів захисту даних, встановлення оновлень програмного забезпечення для безпеки)
- Розслідування інцидентів (запити на розслідування зломів, витоків інформації або інших інцидентів безпеки)
- Навчання і консультації (запити на проведення навчань для співробітників щодо безпечного користування інформаційними системами, консультації щодо кращих практик захисту даних)

У львівському офісі працює менше співробітників порівняно з київським, однак їх кількість зросла після релокації частини персоналу під час війни. Офіс виконує важливі операційні функції, підтримуючи магазини у Західній Україні. Його функції включають операційне управління регіональними магазинами, логістику в Західному регіоні, а також частково підтримку IT та HR функцій. Він є важливим центром для координації регіональних маркетингових кампаній та обслуговування клієнтів.

Завдяки розташуванню у Львові, цей офіс має стратегічний доступ до європейських ринків, що сприяє розширенню співпраці з міжнародними партнерами. Під час війни львівський офіс став ключовим для підтримки безперервності бізнесу та забезпечення стабільної роботи мережі в умовах кризи. Інформаційна безпека у Львові забезпечується через підтримку користувачів на другій лінії підтримки, яка включає прийом заявок та їх усунення. Цей офіс обслуговує орендований сервер parkovy_lviv та активно співпрацює з центральним офісом для координації заходів безпеки та обміну інформацією про потенційні загрози.

До початку повномасштабного вторгнення росії в Україну, у Львові працювали лише працівники групи підтримки, які забезпечували другу лінію підтримки користувачів. Всі основні функції управління та операційна діяльність Групи компаній "Фокстрот" були повністю зосереджені в Києві.

З початком військових дій, з метою забезпечення фізичної безпеки серверів та інших критично важливих інфраструктурних компонентів, було прийнято стратегічне рішення про розгортання серверної інфраструктури у Львові. Це дозволило знизити ризики, пов'язані з фізичними загрозами, та забезпечити безперервність бізнес-процесів.

Також розглядалася можливість оренди серверів у Європі для додаткового підвищення рівня безпеки та стійкості IT-інфраструктури. Проте цей варіант був відхилений через високу вартість таких послуг. У підсумку, було вирішено орендувати сервери в межах України, зокрема сервер parkovy_lviv у Львові та parkovy_kyiv у Києві, що дозволило досягти необхідного рівня безпеки та оптимізувати витрати.

Київський офіс виступає основним центром керування та стратегічного планування для ГК "Фокстрот", забезпечуючи компанію необхідними ресурсами для масштабного розвитку та інновацій. Львівський офіс виконує важливу роль у регіональному управлінні та оперативній підтримці, особливо в умовах кризи. Обидва офіси взаємодоповнюють один одного, сприяючи загальному успіху та стійкості компанії на ринку. Ефективні заходи з інформаційної безпеки, впроваджені в обох локаціях, забезпечують захист даних та надійну роботу інформаційних систем.

2.3. Аналіз практик інформаційної безпеки в групі компаній «Foxtrot»

Головна мета інформаційної безпеки в ГК «Foxtrot» – забезпечення безпеки інформаційних активів та безперервності діяльності бізнесу за рахунок

впровадження системи управління інформаційною безпекою (СУІБ), грамотної експлуатації засобів захисту інформації (ЗЗІ) та адекватного реагування на інциденти інформаційної безпеки. Це досягається через впровадження комплексного підходу до захисту інформації, який включає регулярне оновлення систем, моніторинг загроз, управління доступом та автентифікацію користувачів.

У зв'язку з постійними загрозами кібератак, зростаючими вимогами до збереження конфіденційності даних та необхідністю забезпечення безперебійної роботи бізнес-процесів, «Foxtrot» впроваджує численні заходи для захисту своїх інформаційних систем. Інформація про ці заходи була отримана з програмного забезпечення, розробленого спеціально для ГК «Foxtrot» — «Typhoon», та з інтерв'ю (Додаток Б) з керівником відділу інформаційної безпеки Олексієм Пащенком (рис 6).

2.3.1. Організаційна структура та ключові ролі в інформаційній безпеці

Відділ інформаційної безпеки знаходиться в штаті управляючої компанії Групи компаній «Foxtrot». У відділі працюють два працівника – керівник відділу та менеджер із захисту інформації. Всі функції та процеси, пов'язані з інформаційною безпекою, розподілені між цими працівниками. Основні функції відділу включають організацію та координацію робіт, впровадження та експлуатацію засобів захисту інформації, дослідження технологій обробки інформації з метою виявлення можливих загроз, інвентаризацію інформаційних активів, впровадження та підтримку систем моніторингу, розробку нормативних документів, планування та організацію робіт із залученням підрядних організацій, тестування безпеки програмних комплексів, підвищення обізнаності працівників та участь у розслідуванні інцидентів.

2.3.2.Використання моделей захисту інформацій

У Групі компаній «Фокстрот» активно використовуєтьяс модель управління доступом на основі ролей (Role-Based Access Control, RBAC), яка є ключовим інструментом для забезпечення інформаційної безпеки. Ця модель дозволяє ефективно контролювати доступ до інформаційних ресурсів, базуючись на ролях, які визначаються для кожного співробітника відповідно до їхніх службових обов'язків.

Спочатку аналізуються всі посади для визначення конкретних функціональних обов'язків і необхідних для їх виконання доступів. На основі цього аналізу створюються ролі, які об'єднують набір дозволів для кожної категорії співробітників. Роль «Менеджера з продажів» включає доступ до системи управління взаємовідносинами з клієнтами (CRM), де можна переглядати та оновлювати інформацію про клієнтів, але не мати доступу до фінансових даних компанії. Роль «Бухгалтер» включає доступ до фінансової системи для обліку та звітності, але не надає доступ до конфіденційних даних клієнтів. Роль «IT-спеціаліст» включає доступ до серверної інфраструктури та систем адміністрування, але обмежується в доступі до даних співробітників і клієнтів.

При прийомі на роботу або зміні посади співробітнику автоматично призначається відповідна роль, що спрощує процес управління доступом. При зміні службових обов'язків або проєктних завдань ролі можуть динамічно змінюватися відповідно до нових потреб. Доступ до ресурсів, систем і даних надається на основі призначених ролей, що мінімізує ризики несанкціонованого доступу та забезпечує, що співробітники мають доступ лише до тих ресурсів, які необхідні для виконання їхніх обов'язків.

У ГК «Фокстрот» проводяться регулярні аудити доступів для перевірки відповідності призначених ролей поточним обов'язкам співробітників і для виявлення потенційних порушень. Постійний моніторинг дій користувачів у

системі дозволяє виявляти підозрілу активність і потенційні загрози. Регулярний аудит включає перевірку всіх призначених ролей та дозволів, щоб переконатися, що вони відповідають фактичним обов'язкам співробітників. Це допомагає виявляти надлишкові або застарілі дозволи і своєчасно їх відкликати.

У разі зміни службових обов'язків, звільнення або переведення співробітника роль може бути швидко змінена або видалена, що забезпечує оперативне управління доступами. Права доступу розподіляються та контролюються централізовано, що забезпечує єдність і узгодженість політики безпеки.

2.3.3. Впровадження стандартів ISO

Компанія «Foxtrot» намагається дотримуватись вимог серії стандартів ISO/IEC 27000 у своїй роботі. Хоча прямі вимоги щодо обов'язкового дотримання цих стандартів у галузі наразі відсутні, компанія орієнтується на них як на кращі практики, що допомагають забезпечити високий рівень інформаційної безпеки.

2.3.4. Моніторинг та аналіз загроз

Для моніторингу та аналізу потенційних загроз інформаційній безпеці у «Foxtrot» впроваджено комплексний набір систем захисту, включаючи Next Generation Firewall, корпоративну систему Endpoint Detection and Response, Email Security Appliance, Web Application Firewall, систему управління вразливостями (сканер вразливостей), SIEM-систему, DLP-систему. Моніторинг подій інформаційної безпеки в IT-інфраструктурі делеговано на аутсорсинг комерційному Security Operation Center (SOC). Ці системи дозволяють своєчасно виявляти, аналізувати та блокувати загрози, забезпечуючи надійний захист інформаційних активів компанії. (рис.6)

Рис.6 Скан вразливостей серверів

2.3.5.Регулярні аудити

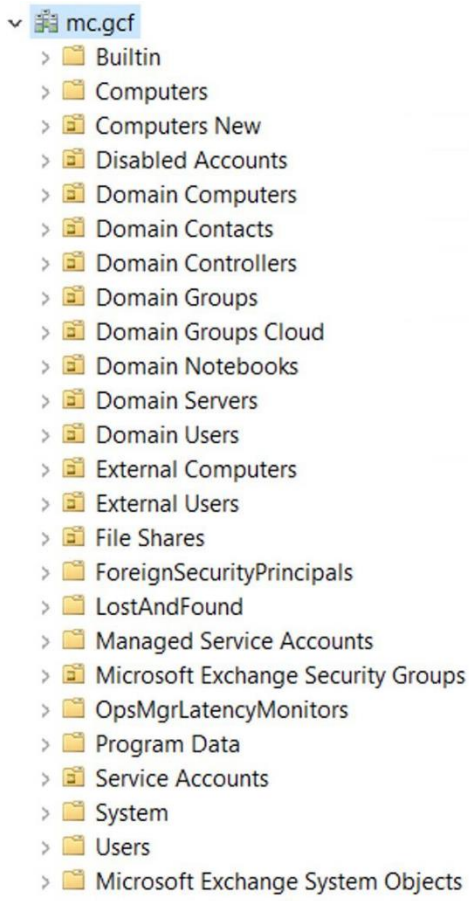
У «Foxtrot» проводяться періодичні зовнішні загальні аудити безпеки, регламент яких не встановлено, та внутрішні аудити, які проводяться внутрішнім відділом інформаційної безпеки в рамках робочих процесів. Ці аудити допомагають оцінити стан безпеки інформаційних систем та виявити можливі вразливості для їх усунення.

2.3.6. Фізична безпека

Фізична безпека конфіденційної інформації знаходиться в компетенції служби безпеки компанії. Інформаційна безпека адмініструє систему контролю доступу, яка включає адміністрування доступу до режимних приміщень, таких як серверні та комутаційні приміщення. Це забезпечує контроль за фізичним доступом до критичних інформаційних активів.

2.3.7.Автентифікація користувачів

У «Foxtrot» розгорнута служба Windows Active Directory, яка забезпечує автентифікацію користувачів у більшості корпоративних додатків та систем. В



системах з підвищеним рівнем критичності або для облікових записів з привілейованими правами використовується багатофакторна автентифікація (MFA). Це дозволяє значно підвищити рівень безпеки та знизити ризики несанкціонованого доступу до конфіденційних даних. (рис.7)

Рис.7 Розгорнута служба Windows Active Directory у ГК «Фокстрот»

2.3.8. Політики та процедури класифікації інформації

У «Foxtrot» існує набір внутрішніх політик та процедур, пов'язаних з інформаційною безпекою. Наприклад, політика інформаційної безпеки, положення про оцінювання та класифікацію інформації, положення про управління інформаційними активами. Ці документи регламентують

класифікацію, обробку та утилізацію конфіденційної інформації, забезпечуючи її захист протягом усього життєвого циклу.

2.3.9. Тренінги та підвищення обізнаності

У компанії проводяться регулярні тренінги та програми підвищення обізнаності для працівників щодо найкращих практик інформаційної безпеки. Періодичні розсилки інформують та нагадують працівникам про основні вимоги інформаційної безпеки, а також їхні ролі та обов’язки щодо захисту конфіденційних даних. Це сприяє формуванню культури безпеки серед співробітників та мінімізує ризики, пов'язані з людським фактором.

2.3.10. Реагування на інциденти

У «Foxtrot» розроблені правила реагування на типові події інформаційної безпеки, які виявляються за допомогою Security Operation Center. За координацію дій та виконання таких правил відповідає відділ інформаційної безпеки. Нетипові інциденти вимагають проведення додаткового розслідування з залученням необхідних співробітників з різних підрозділів, таких як служба безпеки та юридичний департамент. Це забезпечує оперативне та ефективне реагування на інциденти, мінімізуючи їхній вплив на бізнес-процеси.

2.3.11. Передача інформації зовнішнім особам

Для захисту інформації під час її передачі зовнішнім особам, таким як постачальники, партнери чи клієнти, у «Foxtrot» можуть використовуватися різні методи та вимоги, які формуються окремо для різних випадків в залежності від бізнес-процесу або критичності інформації. Це дозволяє забезпечити безпеку інформації під час її передачі, знижуючи ризики витоків та несанкціонованого доступу. [45]

2.3.12. Стратегії резервного копіювання та аварійного відновлення

У «Foxtrot» розробляються, впроваджуються та тестуються плани забезпечення безперервності бізнесу (BCP) та плани аварійного відновлення

(DRP), які визначають порядок та послідовність дій у разі виникнення інциденту, що потребує активації плану. Відповідальним за розроблення та тестування планів є відділ інформаційної безпеки. Це дозволяє компанії забезпечити безперервність бізнесу та захист від втрати даних у разі інциденту безпеки або збою системи.

2.4. Порівняльний аналіз практик безпеки в різних регіонах

Кожен з офісів виконує свої специфічні функції та стикається з різними викликами, що потребує особливих підходів до управління інформаційною безпекою.

Центральний офіс у Києві відповідає за всі ключові функції управління інформаційною безпекою групи компаній. Він здійснює стратегічне планування, координацію заходів безпеки, моніторинг загроз, управління доступом та автентифікацією користувачів, а також регулярні аудити безпеки. Центральний офіс стикається з більшою кількістю хакерських атак, особливо в умовах війни. Це обумовлює необхідність постійного моніторингу та швидкого реагування на інциденти. Моніторинг подій інформаційної безпеки в IT-інфраструктурі делегований на аутсорсинг комерційному Security Operation Center (SOC). На основі інтерв’ю були досліджені системи моніторингу, а також розглянуто кейси їх використання. [48]

Next Generation Firewall (NGFW): NGFW — це вдосконалений тип міжмережевого екрану, який надає додаткові можливості для виявлення та запобігання загрозам. NGFW об'єднує класичні функції міжмережевого екрану з можливостями глибокої перевірки пакетів даних, ідентифікацією додатків та інтелектуальним аналізом загроз. Під час однієї з хакерських атак NGFW дозволив швидко виявити та заблокувати підозрілий трафік, що надходив від зовнішніх IP-адрес, які раніше були позначені як потенційно небезпечні. Це запобігло проникненню шкідливого ПЗ в корпоративну мережу.

Корпоративна система Endpoint Detection and Response (EDR): EDR-системи забезпечують моніторинг, виявлення та реагування на загрози на

кінцевих точках, таких як комп'ютери, мобільні пристрої та сервери. Вони дозволяють виявляти складні загрози, включаючи ті, що обходять традиційні антивірусні програми. Система EDR допомогла виявити та ізолювати кінцеву точку, на яку було встановлено шкідливе програмне забезпечення через фішинговий лист. Це дозволило швидко усунути загрозу без значних втрат даних.

Email Security Appliance (ESA): ESA — це спеціалізоване рішення для захисту електронної пошти, яке забезпечує фільтрацію спаму, виявлення та блокування фішингових атак, а також захист від шкідливого ПЗ. Під час спроби масової фішингової атаки ESA автоматично виявила та заблокувала сотні підозрілих листів, що містили шкідливі посилання та вкладення, захистивши співробітників від потенційних загроз.

Web Application Firewall (WAF): WAF захищає веб-додатки від різних типів атак, таких як SQL-ін'єкції, XSS (міжсайтовий скриптинг) та DDoS-атаки, шляхом фільтрації, моніторингу та блокування HTTP-трафіку до та від веб-додатків.

Система управління вразливостями (Vulnerability Management System): Ця система здійснює регулярне сканування IT-інфраструктури на наявність вразливостей, генерує звіти та допомагає пріоритезувати заходи з усунення виявлених проблем. Після чергового сканування було виявлено критичну вразливість у програмному забезпеченні одного з серверів. Завдяки швидкому реагуванню та встановленню відповідних патчів вдалося запобігти можливому використанню цієї вразливості зловмисниками.

SIEM-система (Security Information and Event Management): SIEM-система об'єднує та аналізує журнали подій з різних джерел для виявлення та реагування на інциденти безпеки в реальному часі. SIEM-система допомогла виявити аномальну активність в мережі, що свідчила про підготовку до внутрішньої атаки. Завдяки швидкому аналізу та реагуванню вдалося запобігти витоку даних.

DLP-система (Data Loss Prevention): DLP-система забезпечує захист від витоку конфіденційної інформації шляхом моніторингу та контролю над передачею даних як всередині компанії, так і за її межами. DLP-система виявила спробу несанкціонованого копіювання конфіденційних даних на зовнішній носій. Це дозволило запобігти втраті даних та провести внутрішнє розслідування інциденту.

Західний офіс у Львові виконує функції підтримки користувачів та управління серверною інфраструктурою. Він зосереджений на оперативному усуненні технічних проблем, реалізації заходів з усунення вразливостей та забезпеченні безперервності роботи бізнес-процесів. Умови війни сприяли перенесенню частини серверної інфраструктури до Західного офісу, що дозволило підвищити фізичну безпеку даних. Проте цей офіс стикається з іншими викликами, такими як необхідність забезпечення безперебійного доступу до ресурсів для працівників та підтримка стабільної роботи серверів під час евакуації.

Центральний офіс часто стикається з масованими хакерськими атаками. Наприклад, в одному з випадків була спроба масового розповсюдження шкідливого ПЗ через фішингові листи. Виявлення та блокування цих листів, а також швидке реагування на інцидент, дозволило запобігти значним втратам даних. (Додаток В)

Західний офіс, у свою чергу, зіткнувся з проблемою недостатньої потужності під час пікового навантаження через евакуацію працівників з Центрального офісу. Це вимагало негайного масштабування серверної інфраструктури та впровадження нових рішень для забезпечення безперебійної роботи систем.

Для оцінки ефективності заходів з інформаційної безпеки, та виявлення слабких місць для прийняття рішення щодо вдосконалення системи захисту інформації, використовуються формули, які базуються на загальноприйнятих стандартах та методиках у цій галузі. [41] Ці стандарти забезпечують методологічну основу для використання таких показників:

1. Коефіцієнт ефективності усунення вразливостей (KEUV): Використовується для вимірювання здатності організації виявляти та усувати вразливості.

2. Середній час реагування на інциденти (STRI): Показує, наскільки швидко команда реагує на інциденти безпеки.

3. Коефіцієнт відновлення даних (KVD): Відображає здатність організації відновлювати дані після інцидентів.

Для вирахування цих показників, використовувалися дані, надані працівником департаменту інформаційних технологій другої лінії підтримки ТОВ «ЕНТРІ» Олександром Робенком, за період з 20.11.2023 по 04.02.2024.

Коефіцієнт ефективності усунення вразливостей (KEUV):

$$KEUV = \frac{\text{Кількість усунених вразливостей}}{\text{Загальна кількість усунених вразливостей}} \times 100\%$$

За вказаний період у Центральному офісі було виявлено 632 вразливості, з яких критичних - 142 , з яких усунено 581 (критичні – усунуто всі), тоді як у Західному офісі було виявлено 50 вразливостей, з яких усунено 47 (за вказаний період критичні вразливості були відсутні). Таким чином, KEUV у Центральному офісі становить:

$$\text{KEUV} = \frac{581}{632} \times 100\% \approx 92\%$$

А KEUV у Західному офісі:

$$\text{KEUV} = \frac{47}{50} \times 100\% \approx 94\%$$

Середній час реагування на інциденти (STRI):

$$STRI = \frac{\sum \text{Час реагування на інцидент}}{\text{Кількість індидентів}}$$

У Центральному офісі за той самий період загальний час реагування на 253 інциденти склав 120 годин, а у Західному офісі на 105 інцидентів – 45 годину. Таким чином, STRI у Центральному офісі становить:

$$STRI = \frac{120}{253} \approx 0.5 \text{ години}$$

А у Західному офісі:

$$STRI = \frac{45}{105} \approx 0.4 \text{ години}$$

Коефіцієнт відновлення даних (KVD):

$$KVD = \frac{\text{Обсяг успішно відновлених даних}}{\text{Обсяг втрачених даних}} \times 100\%$$

У Центральному офісі було втрачено 1.4 ТБ даних, проте завдяки щоденним бекапам вдалося відновити усі дані. У Західному офісі було втрачено 214 ГБ даних, проте через переїзд інфраструктури, з них не вдалося відновити 13 ГБ даних. Таким чином, KVD у Центральному офісі становить:

$$KVD = \sim \frac{1433}{1433} \times 100\% = 100\%$$

А у Західному офісі:

$$KVD = \frac{201}{214} \times 100\% \approx 94\%$$

Ці дані показують, що Західний офіс реагує на інциденти швидше, з середнім часом реагування близько 24-25 хвилин на інцидент, у той час як у Центральному офісі цей час становить приблизно 30 хвилин на інцидент. Це може бути зумовлено більшою кількістю інцидентів у Центральному офісі, проте у порівнянні Центральний офіс має вищий коефіцієнт відновлення даних (100%), що свідчить про ефективнішу систему резервного копіювання та відновлення порівняно із Західним офісом (94%). Це може бути результатом переїзду критичної інфраструктури та більшої уваги до заходів із забезпечення безпеки даних у Центральному офісі.

Висновки до розділу 2: Другий розділ наукової роботи надає глибокий аналіз інформаційної безпеки у центральному офісі в Києві та західному офісі у Львові групи компаній «Фокстрот». Відповідно до проведеного дослідження, розглянуто політики доступу, процедури автентифікації та авторизації,

обізнаність співробітників щодо загроз інформаційній безпеці, а також вплив технічної інфраструктури та регіональних кіберзагроз.

Центральний офіс у Києві, завдяки своїм стратегічним функціям та розвиненій інфраструктурі, виконує ключову роль у забезпеченні інформаційної безпеки компанії, впроваджуючи сучасні заходи захисту та регулярно проводячи аудити безпеки. Впроваджено такі системи, як багатофакторна автентифікація, антивірусні системи та засоби моніторингу загроз, що дозволяють швидко реагувати на інциденти безпеки.

Західний офіс у Львові забезпечує оперативну підтримку користувачів та управління серверною інфраструктурою, зосереджуючись на усуненні технічних проблем та реалізації заходів з усунення вразливостей. Під час війни цей офіс став ключовим для забезпечення безперервності бізнесу та стабільної роботи мережі.

Порівняльний аналіз показує, що кожен офіс стикається зі своїми унікальними викликами, проте завдяки впровадженню сучасних заходів захисту, моніторингу загроз та регулярним аудитам, компанія ефективно захищає свої інформаційні активи. Постійне навчання співробітників і використання найкращих практик забезпечує високий рівень інформаційної безпеки та мінімізує ризики, пов'язані з людським фактором. Це дозволяє компанії зберігати стійкість та адаптивність в умовах сучасних кіберзагроз.

РОЗДІЛ 3. МЕТОДИЧНІ ПІДХОДИ ТА ВПРОВАДЖЕННЯ НОВИХ ПРАКТИК ЗАХИСТУ ІНФОРМАЦІЇ У ГРУПІ КОМПАНІЙ «ФОКСТРОТ»

Цей розділ присвячений аналізу методичних підходів та впровадженню нових практик захисту інформації у групі компаній «Фокстрот». Він охоплює розробку рекомендацій і конкретних заходів для покращення захисту даних, зокрема, удосконалення систем автентифікації, авторизації, шифрування даних та управління доступом. Особлива увага приділяється підвищенню обізнаності співробітників щодо методів соціальної інженерії. Розділ також містить рекомендації на основі міжнародного досвіду та стандартів для підвищення ефективності інформаційної безпеки в компанії.

3.1. Впровадження нових практик захисту інформації

Впровадження нових практик захисту інформації в компанії «Фокстрот» є важливим кроком для забезпечення її безперебійної роботи та захисту від зростаючих кіберзагроз. Це необхідно для зменшення ризиків витоку конфіденційних даних, що може призвести до фінансових втрат і втрати репутації.

Сучасні кіберзагрози постійно еволюціонують, тому організації повинні адаптувати свої системи захисту. Нові практики дозволяють ефективніше виявляти, запобігати і реагувати на загрози, забезпечуючи безпеку інформаційних активів компанії. Це також допомагає зміцнити репутацію «Фокстроту» як надійного партнера, сприяючи залученню нових клієнтів і збереженню існуючих.

Законодавство у сфері захисту даних постійно змінюється і стає жорсткішим. Впровадження нових практик допоможе «Фокстроту» відповідати вимогам, таким як GDPR, що зменшить ризики штрафів і юридичних проблем.

Сучасні практики включають автоматизацію багатьох процесів, що знижує навантаження на IT-персонал і підвищує ефективність роботи. Це сприяє

швидшому реагуванню на інциденти та зменшенню їхнього впливу на бізнес. Кібератаки можуть призвести до значних фінансових втрат, і нові практики допоможуть зменшити ймовірність таких інцидентів та мінімізувати фінансові втрати.

3.1.1. Покращення систем автентифікації та авторизації

Поточна система автентифікації "Фокстроту" в основному спирається на традиційні комбінації імені користувача та пароля. Для авторизації компанія використовує базову модель RBAC, призначаючи права доступу на основі ролей користувачів. Хоча ці методи є стандартними, вони мають кілька вразливостей, включаючи сприйнятливість до зламів паролів, фішинг-атак та внутрішніх загроз. Паролі часто є слабкими, повторно використовуваними або легко вгадуваними, що робить їх основною мішенню для кібератак. Співробітники можуть стати жертвами фішинг-шахрайства, що компрометує їхні облікові дані. Базовий RBAC не достатньо враховує ризик, який представляють незадоволені співробітники або ті, хто зловживає своїми підвищеними привілеями. Використання лише паролів для автентифікації створює єдину точку відмови, що ставить під загрозу всю систему в разі компрометації.

MFA додає додатковий рівень безпеки, вимагаючи від користувачів надання двох або більше факторів перевірки для доступу. Ці фактори зазвичай включають щось, що знає користувач (пароль), щось, що має користувач (смартфон або токен безпеки), і щось, що є користувачем (біометричні дані). Інтегрувати MFA можна з використанням комбінації кодів на основі SMS, додатків для автентифікації та апаратних токенів. Це значно знижує ризик несанкціонованого доступу, забезпечуючи, що скомпрометованих паролів недостатньо для отримання доступу.

3.1.2. Впровадження нових засобів шифрування даних

Поточна система шифрування у "Фокстроті" значною мірою покладалася на традиційні методи, які часто були вразливими через слабкі алгоритми або

неналежне управління ключами. Це залишало дані вразливими до зломів і несанкціонованого доступу. Стандарт шифрування Advanced Encryption Standard (AES) є симетричним алгоритмом, визнаним за його надійність. AES-256, зокрема, забезпечує високий рівень безпеки завдяки довжині ключа в 256 біт, що робить його стійким до атак перебору. Впровадження AES-256 у "Фокстрот" передбачає інтеграцію цього алгоритму в бази даних, системи зберігання файлів та рішення для резервного копіювання, забезпечуючи надійне шифрування всіх конфіденційних даних у стані спокою.

Для захисту даних під час передачі "Фокстрот" впроваджує новітні протоколи TLS. Протоколи Secure Sockets Layer (SSL) та Transport Layer Security (TLS) призначені для забезпечення безпечного зв'язку через комп'ютерну мережу. TLS, спадкоємець SSL, є більш безпечним варіантом, причому версії TLS 1.2 та TLS 1.3 пропонують покращені функції безпеки. Це гарантує, що дані, які обмінюються між системами та з зовнішніми сторонами, зашифровані та захищені від перехоплення і втручання. Налаштування веб-серверів, поштових систем та інших комунікаційних платформ на використання TLS 1.2 або TLS 1.3 дозволяє забезпечити безпеку даних під час передачі.

Апаратне шифрування пропонує кілька переваг над програмними рішеннями. Воно є швидшим, оскільки процес шифрування виконується спеціалізованим обладнанням, а не основним процесором, що зменшує вплив на продуктивність систем і дозволяє здійснювати шифрування та дешифрування в реальному часі. Крім того, апаратне шифрування зазвичай є більш безпечним, оскільки менш вразливе до атак на основі програмного забезпечення і втручання. "Фокстрот" планує інтегрувати апаратне шифрування через використання самошифрувальних накопичувачів (SED) і апаратних модулів безпеки (HSM). SED автоматично шифрують всі дані, записані на диск, забезпечуючи захист навіть у разі фізичного викрадення накопичувача. HSM забезпечують безпечне управління ключами та криптографічні операції, що додатково підвищує безпеку зашифрованих даних.

Повне шифрування диска (FDE) захищає всі дані на диску шляхом шифрування всього накопичувача, включаючи операційну систему. Це гарантує, що дані захищені від несанкціонованого доступу, навіть якщо фізичний диск вилучено та підключено до іншого пристрою. Впровадження FDE у "Фокстрот" передбачає розгортання програмного забезпечення для шифрування, такого як BitLocker або FileVault, на всіх пристроях компанії. Це гарантує захист конфіденційної інформації незалежно від місця її зберігання на диску. FDE особливо корисне для захисту ноутбуків і мобільних пристроїв, які мають більшу ймовірність бути втраченими або викраденими.

Попередні методи шифрування у "Фокстроті" виявилися неефективними через кілька факторів. Слабкі алгоритми шифрування, такі як DES або застарілі версії SSL, забезпечували недостатній захист від сучасних загроз. Неналежні практики управління ключами та відсутність шифрування даних під час передачі додатково піддавали компанію ризикам. Ці методи не відповідали вимогам сучасного ландшафту загроз, залишаючи дані вразливими до зломів та несанкціонованого доступу.

Впровадження передових технологій шифрування у "Фокстроті" приносить кілька значних переваг. AES-256 забезпечує надійний захист даних у стані спокою, що робить їх майже неможливими для розшифрування без ключа. TLS 1.2 і 1.3 гарантують безпечні канали зв'язку, захищаючи дані під час передачі від перехоплення та втручання. Апаратне шифрування пропонує покращену безпеку та продуктивність, тоді як FDE забезпечує комплексний захист усіх даних на пристрої. Впровадження цих інновацій дозволяє "Фокстроту" значно знизити ризик зломів даних, захистити конфіденційну інформацію та відповідати регуляторним вимогам. Ці заходи також підвищують довіру клієнтів та захищають репутацію компанії, демонструючи сильну прихильність до безпеки даних.

3.1.3. Удосконалення політик доступу та управління даними

Поточні політики доступу ГК «Фокстрот» включають стандартні процедури автентифікації та авторизації, які можуть бути недостатньо ефективними для протидії сучасним кіберзагрозам. Існуючі методи автентифікації, зокрема використання комбінації імені користувача та пароля, доповнюються керуванням правами доступу на основі ролей (RBAC). Для підвищення рівня безпеки пропонується впровадження принципу найменших привілеїв, що забезпечує надання користувачам лише мінімальних прав доступу, необхідних для виконання їхніх службових обов'язків. Це значно знижує ризик несанкціонованого доступу до даних. Перегляд та переоцінка ролей і дозволів, регулярні перевірки доступу користувачів, а також автоматизоване управління правами доступу сприятимуть дотриманню цього принципу.

Сегментація мережі, яка розділяє мережу на менші, ізольовані сегменти, обмежить поширення кіберзагроз та утримує потенційні порушення в межах одного сегменту. Розробка стратегії сегментації, впровадження строгих засобів контролю доступу між сегментами та встановлення засобів моніторингу для виявлення та реагування на спроби несанкціонованого доступу допоможуть підвищити загальний рівень безпеки мережі.

Розробка та впровадження чітких політик управління даними, що регулюють доступ, обробку та зберігання даних, є важливим кроком до підвищення інформаційної безпеки. Створення стандартизованих протоколів для запиту та надання доступу до конфіденційних даних, впровадження багаторівневої системи схвалення доступу до критичної інформації та призначення тимчасового доступу забезпечать кращий контроль над даними. Визначення керівних принципів обробки даних, використання сильних алгоритмів шифрування та регулярні аудити діяльності сприятимуть захисту даних на всіх етапах їх життєвого циклу.

Постійний моніторинг доступу до критичних даних у реальному часі дозволить своєчасно виявляти підозрілу активність. Журналювання дій користувачів, використання засобів виявлення аномалій та налаштування автоматизованих оповіщень про підозрілу активність сприятимуть

оперативному реагуванню на можливі загрози. Регулярні аудити журналів доступу та дій користувачів допоможуть виявляти та усувати потенційні проблеми безпеки, забезпечуючи відповідність політикам доступу.

Удосконалення політик доступу та управління даними у ГК «Фокстрот» є критично важливим для підтримки надійної інформаційної безпеки. Впровадження принципу найменших привілеїв, сегментації мережі та всебічних політик управління даними, а також встановлення ефективних методів моніторингу та аудиту дозволить значно покращити контроль та безпеку даних. Ці заходи не лише захистять конфіденційну інформацію, але й підвищать загальну ефективність та надійність інформаційних систем організації.

3.2. Проєкт «Впровадження Ivanti у практики захисту інформації в групі компаній «Фокстрот»

Зважаючи необхідність забезпечення високого рівня безпеки інформації, керівник відділу IT-інфраструктури прийняв рішення впровадити у діяльність групи компаній «Фокстрот» рішення Ivanti. Це дозволить значно підвищити захист аналітичних даних користувачів, зокрема працівників та покупців, і забезпечити ефективне управління IT-ресурсами. У своїй науковій роботі я пропоную проєкт впровадження системи Ivanti, що включає детальний план дій та розрахунки, необхідні для успішної реалізації цього проєкту. Це дозволить організації не тільки зміцнити інформаційну безпеку, але й підвищити загальну ефективність операційних процесів. [58]

3.3.1. Мета та завдання проєкту, огляд рішень Ivanti

План реалізації має важливе значення для виявлення та пом’якшення ризиків безпеки, підвищення стану безпеки організації та забезпечення дотримання нормативних вимог. Він оптимізує та стандартизує методи безпеки, захищаючи бізнес-активи та сприяючи культурі безпеки серед співробітників. План підтримує безперервне вдосконалення, безперервність бізнесу та зміцнює довіру клієнтів і партнерів. Відповідаючи стратегічним цілям організації, план

гарантує, що заходи безпеки підтримують і сприяють зростанню бізнесу та інноваціям.

Метою даного проєкту є впровадження системи захисту інформації в організації за допомогою рішень Ivanti. Це дозволить забезпечити високий рівень безпеки даних, мінімізувати ризики витоку інформації та кіберзагроз, а також покращити загальну ефективність управління IT-ресурсами.

Ivanti — це провідна компанія, що надає рішення для управління IT-активами та сервісами. Вона пропонує комплексний підхід до забезпечення безпеки інформації, управління конфігураціями, оновленням програмного забезпечення та захистом кінцевих точок. Продукти Ivanti дозволяють автоматизувати багато процесів, що значно спрощує роботу IT-відділів та підвищує рівень безпеки організації.

Ivanti автоматизує процеси оновлення програмного забезпечення для забезпечення актуальності та безпеки систем, забезпечує захист пристроїв від вірусів, шкідливого ПЗ та несанкціонованого доступу, виявляє та усуває вразливості у програмному забезпеченні та системах, надає тільки авторизованим користувачам доступ до критично важливої інформації, забезпечує шифрування та запобігання витоку конфіденційних даних, а також миттєво виявляє кіберзагрози та оперативно реагує на них.

Впровадження рішень Ivanti в організації дозволяє досягти таких переваг: підвищення рівня безпеки завдяки автоматизованим процесам управління безпекою та оновленням, швидка реакція на нові загрози та мінімізація ризиків, ефективне управління ресурсами завдяки автоматизації багатьох рутинних завдань, що дозволяє IT-відділу зосередитися на стратегічних питаннях та підвищити загальну продуктивність. Це також сприяє зниженню витрат завдяки впровадженню єдиної платформи для управління безпекою та IT-ресурсами, що дозволяє знизити витрати на підтримку та обслуговування інфраструктури. Крім того, Ivanti допомагає організаціям відповідати вимогам нормативних актів та стандартів у сфері кібербезпеки. [59]

Система пропонує широкий спектр рішень, які допомагають організаціям забезпечити надійний захист інформації та ефективне управління IT-ресурсами. Основні функції та переваги рішень Ivanti включають управління патчами, автоматизацію процесу оновлення програмного забезпечення, що забезпечує актуальність і безпеку систем. Це дозволяє оперативно впроваджувати нові патчі та виправлення, зменшуючи вразливість систем до кіберзагроз. Ivanti також забезпечує захист кінцевих точок, надаючи засоби для захисту пристроїв від вірусів, шкідливого програмного забезпечення та несанкціонованого доступу, що гарантує цілісність та конфіденційність даних на всіх пристроях організації. Рішення Ivanti дозволяють виявляти та усувати вразливості у програмному забезпеченні та системах, що допомагає знизити ризики кіберзагроз та підвищити загальний рівень безпеки. Ivanti надає інструменти для управління доступом до критично важливої інформації, забезпечуючи лише авторизованим користувачам доступ до даних, що запобігає несанкціонованому доступу та витоку інформації. Ivanti також забезпечує шифрування та запобігання витоку конфіденційних даних, включаючи засоби для запобігання витоку інформації (DLP) та забезпечення безпеки даних на всіх етапах.

Ivanti дозволяє миттєво виявляти кіберзагрози та оперативно реагувати на них, що допомагає організаціям швидко вживати заходів для запобігання або мінімізації наслідків кіберінцидентів. Крім того, Ivanti допомагає організаціям відповідати вимогам нормативних актів та стандартів у сфері кібербезпеки, що знижує ризики юридичних та фінансових наслідків. Автоматизація процесів управління IT-ресурсами та безпекою значно спрощує роботу IT-відділів та підвищує загальну ефективність організації.

3.3.2. Потенційні ризики та стратегії управління ними

Проєкт може зіткнутися з затримками через технічні труднощі, затримку в доставці обладнання або інші непередбачені обставини. Для управління цим ризиком необхідно розробити детальний план проєкту з чіткими термінами для кожного етапу, регулярно проводити зустрічі для контролю за дотриманням

графіка, передбачити резервний час для вирішення можливих проблем та затримок, а також розробити план дій на випадок затримок, включаючи швидку ескалацію проблем до вищого керівництва. Співробітники можуть не отримати достатньо знань і навичок для ефективної роботи з новими системами Ivanti, тому важливо забезпечити повний цикл навчання, включаючи теоретичні заняття, практичні тренінги та сертифікацію, а також постійну технічну підтримку і консультації після завершення навчання. Регулярні оцінки знань та навичок співробітників допоможуть виявити та усунути прогалини.

Під час впровадження можуть виникнути технічні проблеми, які вплинуть на роботу систем. Для цього необхідно проводити ретельне попереднє тестування всіх компонентів систем до їхнього впровадження, розробити детальний план дій на випадок технічних проблем, включаючи резервні рішення та запасні частини, а також впровадити систему моніторингу для швидкого виявлення та усунення проблем. Витрати на впровадження можуть перевищити запланований бюджет через непередбачені витрати або інші фактори. Щоб цього уникнути, потрібно впровадити систему регулярного фінансового контролю для відстеження витрат, передбачити резервний фонд для покриття непередбачених витрат та проводити регулярний аналіз витрат для виявлення та усунення можливих перевитрат.

Впровадження систем Ivanti може не забезпечити очікуваної вигоди через неправильне налаштування або використання. Встановлення чітких та вимірюваних цілей впровадження, регулярний моніторинг ефективності використання систем Ivanti та коригуючі заходи у разі виявлення невідповідності між очікуваною та фактичною вигодою допоможуть мінімізувати цей ризик. Завдяки детальному плануванню, регулярному моніторингу, підготовці резервів та впровадженню стратегій управління ризиками, можна мінімізувати їх вплив та забезпечити успішне впровадження систем.

3.3.3. Підготовчий етап впровадження рішень Ivanti

Впровадження рішень Ivanti у компанію, яка займається підтримкою користувачів та IT інфраструктури, є складним та багатоступеневим процесом, що вимагає ретельного планування та підготовки. Основною метою впровадження є забезпечення надійного захисту аналітичних даних, підвищення ефективності управління IT-інфраструктурою та поліпшення якості підтримки користувачів.

Підготовчий етап є критично важливим для успішного впровадження, оскільки він закладає основу для всіх наступних кроків проєкту. Він включає аналіз потреб компанії, визначення вимог до програмного забезпечення та обладнання, розробку детального плану впровадження та підготовку до закупівлі необхідних ресурсів. Даний етап триватиме один місяць, з 1 липня 2024 року по 31 липня 2024 року.

1. Визначення вимог до рішень Ivanti (1 тиждень)

- **Консультації з постачальниками (2 дні)**
  - **Діяльність**: Проведення зустрічей з представниками компанії Ivanti та іншими постачальниками, які пропонують подібні рішення.
  - **Ціль**: Отримання інформації про можливості, функціональність та переваги різних продуктів Ivanti.
  - **Відповідальний**: Керівник IT-відділу.
- **Аналіз вимог компанії (3 дні)**
  - **Діяльність**: Оцінка потреб компанії у сфері захисту аналітичних даних, управління IT-інфраструктурою та підтримки користувачів.
  - **Ціль**: Визначення ключових функціональних вимог до рішень Ivanti.
  - **Відповідальний**: Керівник відділу інформаційної безпеки.
- **Складання технічного завдання (2 дні)**
  - **Діяльність**: Документування технічних та функціональних вимог до рішень Ivanti.
  - **Ціль**: Підготувати чітке та детальне технічне завдання для подальшої реалізації.
  - **Відповідальний**: Менеджер із захисту інформації.

2. Складання детального плану впровадження (2 тижні)

- **Розробка плану впровадження (5 днів)**
  - **Діяльність**: Розробка детального плану впровадження рішень Ivanti, включаючи етапи, терміни, ресурси та відповідальних осіб.
  - **Ціль**: Забезпечити чіткий та структурований підхід до впровадження.
  - **Відповідальний**: Керівник IT-відділу у співпраці з керівником відділу інформаційної безпеки.
- **Узгодження плану з керівництвом та ключовими зацікавленими сторонами (3 дні)**
  - **Діяльність**: Проведення зустрічей з керівництвом компанії та іншими зацікавленими сторонами для обговорення та узгодження плану впровадження.
  - **Ціль**: Отримати підтримку та схвалення плану впровадження від усіх ключових зацікавлених сторін.
  - **Відповідальний**: Керівник IT-відділу.
- **Підготовка фінального документу плану впровадження (2 дні)**
  - **Діяльність**: Внесення змін та доповнень до плану впровадження на основі зворотного зв'язку від зацікавлених сторін.
  - **Ціль**: Підготувати остаточну версію плану впровадження, яка буде затверджена керівництвом.
  - **Відповідальний**: Менеджер із захисту інформації.

3. Закупівля мережевого обладнання та програмного забезпечення (1 тиждень)

- **Проведення тендеру та вибір постачальників (3 дні)**
  - **Діяльність**: Організація та проведення тендеру для вибору постачальників мережевого обладнання та програмного забезпечення.
  - **Ціль**: Вибрати найкращих постачальників, які пропонують якісне обладнання та програмне забезпечення за оптимальною ціною.
  - **Відповідальний**: Керівник IT-відділу.

- **Закупівля та доставка обладнання (4 дні)**
  - **Діяльність**: Оформлення замовлень на закупівлю обладнання та програмного забезпечення, організація доставки до офісу компанії.
  - **Ціль**: Забезпечити своєчасну доставку всіх необхідних компонентів для впровадження.
  - **Відповідальний**: Менеджер із захисту інформації.

3.3.4. Етап впровадження

Етап впровадження триватиме три місяці, з 1 серпня 2024 року по 31 жовтня 2024 року. Протягом цього часу будуть виконані основні завдання, пов’язані з інтеграцією та налаштуванням рішень Ivanti. До цих завдань належать закупівля та встановлення мережевого обладнання, інсталяція та налаштування програмного забезпечення Ivanti, а також інтеграція нових систем з існуючими. Цей етап є надзвичайно важливим, оскільки він забезпечує технічну готовність компанії до роботи з новими інструментами та технологіями, а також створює основу для ефективного управління IT-інфраструктурою та захисту аналітичних даних.

1. Закупівля мережевого обладнання та програмного забезпечення (3 тижні)

- **Проведення тендеру та вибір постачальників (1 тиждень)**
  - **Діяльність**: Організація тендеру для вибору постачальників мережевого обладнання та програмного забезпечення Ivanti.
  - **Ціль**: Вибір оптимальних постачальників за критеріями ціни та якості.
  - **Відповідальний**: Керівник IT-відділу.
- **Оформлення замовлень та доставка (2 тижні)**
  - **Діяльність**: Оформлення замовлень та організація доставки обладнання та програмного забезпечення до офісу компанії.
  - **Ціль**: Забезпечити своєчасну доставку всіх необхідних компонентів.

- **Відповідальний**: Менеджер із захисту інформації.

2. Встановлення мережевого обладнання (3 тижні)

- **Монтаж та налаштування серверів (2 тижні)**
  - **Діяльність**: Встановлення нових серверів та іншого мережевого обладнання в дата-центрі компанії.
  - **Ціль**: Підготувати інфраструктуру для інсталяції програмного забезпечення Ivanti.
  - **Відповідальний**: Команда IT-відділу.
- **Налаштування мережевих з'єднань (1 тиждень)**
  - **Діяльність**: Налаштування мережевих з'єднань та забезпечення стабільного зв'язку між новим обладнанням та існуючою інфраструктурою.
  - **Ціль**: Забезпечити безперебійну роботу мережі.
  - **Відповідальний**: Інженери мережевого відділу.

3. Інсталяція та налаштування програмного забезпечення Ivanti (4 тижні)

- **Інсталяція програмного забезпечення (2 тижні)**
  - **Діяльність**: Інсталяція програмного забезпечення Ivanti на нові сервери.
  - **Ціль**: Забезпечити функціонування всіх необхідних модулів Ivanti.
  - **Відповідальний**: Команда IT-відділу.
- **Налаштування функціоналу (2 тижні)**
  - **Діяльність**: Налаштування програмного забезпечення відповідно до потреб компанії та вимог інформаційної безпеки.
  - **Ціль**: Оптимізувати роботу програмного забезпечення під специфіку компанії.
  - **Відповідальний**: Менеджер із захисту інформації.

4. Інтеграція з існуючими системами (4 тижні)

- **Тестування сумісності (2 тижні)**
  - **Діяльність**: Проведення тестів на сумісність програмного забезпечення Ivanti з існуючими системами.

- **Ціль**: Виявлення та усунення можливих проблем при інтеграції.
- **Відповідальний**: Команда IT-відділу.

- **Налаштування процесів обміну даними (2 тижні)**
  - **Діяльність**: Налаштування процесів обміну даними між новими та існуючими системами.
  - **Ціль**: Забезпечити безперебійний обмін даними для ефективної роботи компанії.
  - **Відповідальний**: Інженери мережевого відділу.

Для забезпечення ефективного впровадження рішень Ivanti необхідно придбати мережеве обладнання, яке відповідатиме вимогам компанії щодо безпеки та продуктивності. Ось детальний план закупівлі обладнання з орієнтовними розрахунками, заснованими на середніх цінах пристроїв з необхідними характеристиками:

1. Сервери

- **Кількість**: 10
- **Орієнтовна вартість одного сервера**: $7,500
- **Загальна вартість серверів**: 10 x $7,500 = $75,000

2. Мережеві комутатори (Switches)

- **Кількість**: 5
- **Орієнтовна вартість одного комутатора**: $3,000
- **Загальна вартість комутаторів**: 5 x $3,000 = $15,000

3. Мережеві маршрутизатори (Routers)

- **Кількість**: 3
- **Орієнтовна вартість одного маршрутизатора**: $2,500
- **Загальна вартість маршрутизаторів**: 3 x $2,500 = $7,500

4. Системи зберігання даних (Storage Systems)

- **Кількість**: 2
- **Орієнтовна вартість однієї системи**: $10,000
- **Загальна вартість систем зберігання даних**: 2 x $10,000 = $20,000

5. Мережеві кабелі та аксесуари

- **Кількість**: Набір для всіх пристроїв
- **Орієнтовна вартість**: $5,000
- **Загальна вартість кабелів та аксесуарів**: $5,000

6. Джерела безперебійного живлення (UPS)

- **Кількість**: 5
- **Орієнтовна вартість одного UPS**: $1,500
- **Загальна вартість UPS**: 5 x $1,500 = $7,500

7. Інші витрати (монтаж, налаштування, доставка)

- **Орієнтовна вартість**: $10,000

Загальні витрати на мережеве обладнання

1. Сервери: $75,000
2. Мережеві комутатори: $15,000
3. Мережеві маршрутизатори: $7,500
4. Системи зберігання даних: $20,000
5. Мережеві кабелі та аксесуари: $5,000
6. Джерела безперебійного живлення: $7,500
7. Інші витрати: $10,000

Загальна вартість мережевого обладнання: $75,000 + $15,000 + $7,500 + $20,000 + $5,000 + $7,500 + $10,000 = **$140,000**

Для проведення тендеру на закупівлю мережевого обладнання та програмного забезпечення можна використовувати кілька популярних платформ:

- ProZorro (https://prozorro.gov.ua/): Державна система електронних закупівель, забезпечує прозорість та відкритість.
- Zakupki.Prom.ua (https://zakupki.prom.ua): Комерційна платформа для електронних торгів та тендерів, інтегрована з ProZorro.
- Tender.Me (https://tender.me/): Платформа для індивідуальних тендерів з можливостями аналітики та звітності.

- SmartTender (https://smarttender.biz/): Повний цикл тендерного процесу з інтуїтивним інтерфейсом та широкими функціональними можливостями.
- eTenders (https://etenders.com.ua/): Платформа для електронних торгів, що забезпечує повну прозорість процесу.

Використання цих платформ забезпечить прозорість та ефективність закупівель для впровадження рішень Ivanti.

3.3.5. Етап навчання співробітників

Етап навчання триватиме з 1 листопада 2024 року по 31 грудня 2024 року та включатиме навчання 150 співробітників підтримки користувачів та підвищення кваліфікації 10 працівників IT-відділу та відділу інформаційної безпеки. Загальна вартість цього етапу складе приблизно $40,000. Основною метою етапу навчання є забезпечення всім співробітникам необхідних знань та навичок для ефективної роботи з новими системами Ivanti та підвищення кваліфікації ключових працівників для ефективного управління та підтримки цих систем.

1. Навчання персоналу роботі з новими системами (4 тижні)

- **Загальна кількість співробітників**: 150 (підтримка користувачів)
- **Формат навчання**:
  - Онлайн-тренінги та вебінари.
  - Очні заняття в тренінговому центрі компанії.
  - Практичні заняття з використанням нових систем Ivanti.
- **Орієнтовна вартість навчання одного співробітника**: $200
- **Загальна вартість навчання персоналу**: 150 x $200 = $30,000
- **Ціль**: Забезпечити всім співробітникам необхідні знання та навички для ефективної роботи з новими системами Ivanti.
- **Відповідальний**: Менеджер із захисту інформації та зовнішні тренери.

2. Підвищення кваліфікації працівників ІТ-відділу та відділу інформаційної безпеки (4 тижні)

- **Загальна кількість співробітників**: 10 (ІТ-відділ та відділ інформаційної безпеки)
- **Формат навчання**:
  - Спеціалізовані курси та сертифікаційні програми з роботи з продуктами Ivanti.
  - Індивідуальні заняття та тренінги.
- **Орієнтовна вартість навчання одного співробітника**: $1,000
- **Загальна вартість підвищення кваліфікації**: 10 x $1,000 = $10,000
- **Ціль**: Підвищити кваліфікацію ключових працівників ІТ-відділу та відділу інформаційної безпеки для забезпечення ефективного управління та підтримки нових систем Ivanti.
- **Відповідальний**: Керівник ІТ-відділу та зовнішні тренери.

Загальні витрати на етап навчання

1. **Навчання персоналу роботі з новими системами**: $30,000
2. **Підвищення кваліфікації працівників ІТ-відділу та відділу інформаційної безпеки**: $10,000

Загальна вартість етапу навчання: $30,000 + $10,000 = **$40,000**

3.3.6. Етап тестування впроваджених рішень

Етап тестування та запуску триватиме з 1 січня 2025 року по 31 січня 2025 року та включатиме три основні підпункти: тестування функціональності та безпеки систем, виправлення виявлених помилок, офіційний запуск рішень Ivanti в експлуатацію. Основною метою цього етапу є забезпечення повної працездатності та безпеки систем, а також їх безперебійного запуску. Загальна вартість етапу складе приблизно $5,000 на непередбачені витрати.

1. Тестування функціональності та безпеки систем (2 тижні)

- **Діяльність**:
  - Проведення внутрішніх тестів для перевірки функціональності всіх компонентів систем Ivanti.

- Проведення тестів на безпеку, включаючи перевірку наявності вразливостей та випробування на стійкість до можливих атак.

- **Ціль**: Забезпечити повну працездатність систем та їх відповідність вимогам безпеки.
- **Відповідальний**: Керівник відділу інформаційної безпеки.

2. Виправлення виявлених помилок (1 тиждень)

- **Діяльність**:
  - Виправлення помилок та проблем, виявлених під час тестування.
  - Повторне тестування виправлених компонентів для підтвердження усунення помилок.
- **Ціль**: Гарантувати стабільну роботу систем після впровадження.
- **Відповідальний**: Команда IT-відділу.

3. Офіційний запуск рішень Ivanti в експлуатацію (1 тиждень)

- **Діяльність**:
  - Підготовка до запуску, включаючи перевірку готовності всіх систем та співробітників.
  - Запуск систем в робочий режим.
  - Моніторинг роботи систем у перші дні після запуску для виявлення та оперативного виправлення можливих проблем.
- **Ціль**: Забезпечити безперебійний запуск та стабільну роботу нових систем Ivanti.
- **Відповідальний**: Керівник IT-відділу та керівник відділу інформаційної безпеки.

Непередбачені витрати у розмірі $5,000 включають резерв на випадок додаткових витрат, пов'язаних з технічними проблемами, додатковими заходами безпеки, залученням зовнішніх консультантів та іншими непередбаченими ситуаціями, які можуть виникнути під час тестування та запуску систем Ivanti. Цей резерв дозволить оперативно вирішувати будь-які проблеми, що виникнуть, забезпечуючи таким чином стабільну та безпечну роботу нових рішень.

Після завершення розробки детального плану впровадження рішень Ivanti в компанії, проект було відправлено працівнику IT-відділу для оцінки та перевірки. Отриманий відгук був надзвичайно позитивним, оскільки працівник високо оцінив структуру, чіткість та детальність представленого плану. Його зауваження та рекомендації підтвердили, що розроблений план відповідає вимогам компанії та враховує всі необхідні аспекти для успішного впровадження рішень Ivanti. Така позитивна оцінка є свідченням того, що підготовлений проект має високі шанси на успішну реалізацію та принесе очікувану користь компанії, забезпечуючи високий рівень інформаційної безпеки та ефективності управління IT-інфраструктурою. (Додаток Г)

Висновки до розділу 3: Основним аспектом даного розділу є впровадження рішень Ivanti, що передбачає комплексний підхід до управління IT-активами та сервісами, включаючи автоматизацію процесів оновлення програмного забезпечення, захист кінцевих точок, управління вразливостями та забезпечення відповідності вимогам нормативних актів. Запропонований план впровадження рішень Ivanti демонструє чітку структуру та детальний підхід до кожного етапу реалізації, включаючи підготовчий етап, закупівлю мережевого обладнання та програмного забезпечення, встановлення та налаштування систем, навчання співробітників та тестування впроваджених рішень.

Важливою частиною розділу є детальний план дій та розрахунки необхідні для успішної реалізації проекту, що включає етапи підготовки, впровадження, навчання та тестування. Впровадження багатофакторної автентифікації (MFA), Advanced Encryption Standard (AES-256), та інших сучасних засобів захисту значно підвищує рівень безпеки інформаційних активів компанії, мінімізуючи ризики несанкціонованого доступу та втрати даних.

Окрему увагу приділено удосконаленню політик доступу та управління даними, що включає впровадження принципу найменших привілеїв, сегментацію мережі, та створення чітких протоколів для запиту та надання доступу до конфіденційних даних. Постійний моніторинг доступу та регулярні

аудити дозволяють своєчасно виявляти та усувати потенційні загрози, забезпечуючи високий рівень контролю над даними.

Розглянуто також питання фізичної безпеки інформаційних активів, що включає адміністрування доступу до режимних приміщень, а також заходи з управління інцидентами та відновлення після аварій, що дозволяють забезпечити безперервність бізнесу навіть у випадку серйозних збоїв.

Впровадження нових практик захисту інформації у групі компаній «Фокстрот» є важливим кроком для забезпечення її безперебійної роботи та захисту від зростаючих кіберзагроз. Ці заходи не тільки підвищують рівень інформаційної безпеки, але й сприяють зміцненню репутації компанії як надійного партнера, що залучає нових клієнтів і зберігає існуючих. Завдяки комплексному підходу до захисту даних, використанню сучасних технологій та регулярному підвищенню обізнаності співробітників, «Фокстрот» здатний ефективно протистояти сучасним кіберзагрозам та підтримувати високий рівень інформаційної безпеки у своїй діяльності.

ВИСНОВКИ

Захист інформації від несанкціонованого доступу у контексті аналітичної культури організації є надзвичайно важливим питанням для сучасних українських організацій. В умовах постійного розвитку інформаційних технологій та зростаючих загроз кібербезпеці, забезпечення належного захисту даних стає ключовим фактором для підтримання стабільності та конкурентоспроможності бізнесу. Ефективні методи захисту інформації повинні включати як технічні рішення, так і організаційні заходи, що сприяють формуванню культури безпеки на всіх рівнях організації.

У першому розділі розглянуто теоретичні основи захисту інформації в контексті аналітичної культури організацій. Було досліджено основні поняття та значення захисту інформації, включаючи визначення та важливість інформаційної безпеки в сучасному цифровому контексті. Аналітична культура

організацій була визначена як критичний фактор, що сприяє прийняттю рішень на основі даних та підвищенню ефективності роботи.

Особлива увага приділялася загрозам для інформаційних систем, які можуть бути як внутрішніми (інсайдерські загрози), так і зовнішніми (кібератаки). Було встановлено, що для ефективного захисту необхідно класифікувати загрози та впроваджувати відповідні заходи безпеки, такі як багатофакторна автентифікація, регулярні оновлення програмного забезпечення та використання сучасних моделей захисту інформації. Моделі захисту інформації, такі як модель Белла-ЛаПадули, модель Біби та модель RBAC, були розглянуті як важливі інструменти для підтримання конфіденційності, цілісності та доступності даних.

Також було досліджено організаційні заходи з захисту інформації, включаючи політики інформаційної безпеки, тренінги з підвищення обізнаності, оцінку та управління ризиками, а також моніторинг та аудит інформаційної безпеки. Ці заходи є критичними для забезпечення захисту інформаційних активів та формування культури безпеки в організаціях.

Другий розділ був присвячений аналізу інформаційної безпеки в центральному та західному офісах групи компаній Foxtrot. Було проведено порівняльний аналіз практик інформаційної безпеки в обох офісах, що дозволило виявити сильні та слабкі сторони кожного з них. Зокрема, було виявлено, що центральний офіс має більш розвинені політики та процедури захисту інформації, тоді як західний офіс демонструє кращі результати у впровадженні стандартів ISO та регулярному моніторингу загроз.

Аналіз практик інформаційної безпеки в групі компаній Foxtrot включав дослідження організаційної структури та ключових ролей в інформаційній безпеці, використання моделей захисту інформації, впровадження стандартів ISO, моніторинг та аналіз загроз, регулярні аудити, фізичну безпеку, автентифікацію користувачів, політики та процедури класифікації інформації, тренінги та підвищення обізнаності, реагування на інциденти, передачу

інформації зовнішнім особам, стратегії резервного копіювання та аварійного відновлення.

Інтерв'ю з працівниками департаменту інформаційних технологій та служби безпеки підтвердили, що існуючі заходи захисту інформації є ефективними, але потребують постійного вдосконалення та адаптації до нових загроз. Було виявлено, що співробітники усвідомлюють важливість інформаційної безпеки та готові підтримувати впровадження нових практик.

Третій розділ був присвячений методичним підходам та впровадженню нових практик захисту інформації в групі компаній Foxtrot. Було розроблено детальний план впровадження рішень Ivanti, який включає закупівлю обладнання, навчання персоналу та тестування систем. Основною метою цього проекту є підвищення рівня захисту інформації шляхом впровадження передових технологій та методик.

Особлива увага була приділена аналізу ризиків та розробці стратегій управління ними. Було визначено потенційні ризики, пов'язані з впровадженням нових технологій, та запропоновано ефективні стратегії їхнього управління. Важливим аспектом проекту є також підготовчий етап, який включає детальне планування та тестування всіх компонентів системи.

На основі проведеного дослідження можна зробити висновок, що захист інформації від несанкціонованого доступу є критичним елементом сучасних організацій, особливо в умовах швидкого розвитку інформаційних технологій та зростаючих загроз кібербезпеці. Аналітична культура організацій відіграє важливу роль у забезпеченні інформаційної безпеки, сприяючи прийняттю рішень на основі даних та формуванню культури безпеки. Впровадження сучасних технологій та методик, таких як рішення Ivanti, дозволяє ефективно захищати інформаційні активи та забезпечувати їхню конфіденційність, цілісність та доступність. Це дослідження підкреслює важливість постійного вдосконалення заходів інформаційної безпеки та адаптації до нових загроз, що є ключовим фактором для успішного функціонування організацій в сучасному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. No 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80.

2. Про захист персональних даних: Закон України від 01.06.2010 р. No 2704-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

3. Про ринки капіталу та організовані товарні ринки: Закон України від 23.02.2006 р. № 3480-IV. URL: https://zakon.rada.gov.ua/laws/show/3480-15#Text.

4. Про Стратегію інформаційної безпеки: Рішення від 15.10.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#n2.

5. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 р. № 1089-IX: станом на 16 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

6. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII: станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

7. Апелло Ю. Менеджмент 3.0. Agile-менеджмент. Львів: Фабула, 2019. 432 с.

8. Баран М. В. Захист інформації у контексті забезпечення інформаційної безпеки. Аналітично-порівняльне правознавство. 2022. № 3.

9. Бобала Ю. Я., Горбатий І. В. Інформаційна безпека. Львів: Львів. політехніка, 2019. 580 с.

10. Борсуковський Ю. В., Бурячок В. Л. Роль і місце вищих навчальних закладів у створенні системи інформаційної та кібернетичної безпеки України. Сучасний захист інформації. 2011. № 4 (184). С. 126–128.

11. Варенко В. М. Аналітика: сучасні тенденції та виклики. Бібліотекознавство. Документознавство. Інформологія. 2019. № 1. С. 118–123.

12. Гребніков В. В. Комплексні системи захисту інформації. проєктування, впровадження, супровід: Зб. лекцій. Ridero, 2018. 380 с.

13. Грей Дж. Соціальна інженерія і етичний хакінг на практиці. Дніпро: Пед. преса, 2022. 226 с.

14. Гриценко О. Суспільство, держава, інформація. Київ: Ін-т журналістики КНУ ім. Т. Шевченка, 2001. 165 с.

15. Джинчарадзе Н. Інформаційна культура: Навч. посіб. для студ. вищ. закл. освіти. Київ, 1999. 148 с.

16. Досенко С. Д. Технічний захист інформації. основні проблеми та способи їх вирішення. Herald of Lviv University of Trade and Economics Technical Sciences. 2021. № 27. С. 27–32. URL: https://doi.org/10.36477/2522-1221-2021-27-04.

17. Ємельянов С. Проблемні аспекти класифікації інформації з обмеженим доступом в Україні. Наукові праці Національного університету "Одеська юридична академія". 2019. Т. 12. С. 130–140. URL: https://doi.org/10.32837/npnuola.v12i0.221.

18. Захист інформації від несанкціонованого доступу: Theses / А. М. Куліш та ін. 2013. URL: http://essuir.sumdu.edu.ua/handle/123456789/31765.

19. Іванюта Т., Заїчковський А. Економічна безпека підприємства. Київ: Центр учб. літ., 2020. 256 с.

20. Касянчук Н. В., Ткачук Л. М. Захист інформації в базах даних: Thesis. 2019. URL: http://ir.lib.vntu.edu.ua//handle/123456789/24448.

21. Кенеді Д. Безжальний менеджмент. Управління людьми та прибутком. Львів: Фабула, 2021. 304 с.

22. Кобко Є.В. Правові засади забезпечення національної безпеки в Україні. Порівняльно-аналітичне право. 2018. № 6. С. 240–243.

23. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній. SIDCON: Київ, 2021. 372 с.

24. Когут Ю. І. Кібервійна та безпека об'єктів критичної інфраструктури: Практ. посіб. Київ: SIDCON, 2021. 332 с.

25. Колінз М. Захист мереж. Підхід на основі аналізу даних. Харків: O'Reilly, 2020. 308 с.

26. Кононович В. Г. Соціальний захист інформації в класах систем захисту інформації. Ukrainian Information Security Research Journal. 2008. Т. 10, № 4(41). URL: https://doi.org/10.18372/2410-7840.10.3870.

27. Коц Д. В. Система нормативно-правових актів, що регулюють захист інформації з обмеженим доступом. Порівняльно-аналітичне право. 2020. № 1. С. 343–346.

28. Коц Д. В. Становлення й розвиток системи захисту інформації з обмеженим доступом в Україні (1991–2019 рр.). Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2019. № 3 (43).

29. Кузнєцов В. І. Українська аналітика науки: спроба метааналізу. Філософська думка. 2008. № 2. С. 15–50.

30. Ліпкан В.А. Національна безпека України: навч. посібник. Київ: КНТ, 2009. 576 с.

31. Лісовська Ю. П., Лісовський П. М. Захист інформації: міжнародні відносини та політичний консалтинг: Навч. посіб. Київ: Ліра-К, 2022. 312 с.

32. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації: Навч. посіб. Одеса: Фенікс, 2015. 264 с.

33. Максимець В., Свірідова Т. Трансформація політичних виборчих кампаній в еру Big-data технологій. Міжнародні відносини, суспільні комунікації та регіональні студії. 2019. № 2.

34. Мандзюк О. А. Правовий потенціал поняття «аналітика». Актуальні проблеми держави і права. 2020. № 84. URL: https://doi.org/10.32837/apdp.v0i84.148.

35. Мехед Д. Б. Захист інформації на підприємстві. Вісник Чернігівського державного технологічного університету. Серія "Технічні науки". 2014. № 2 (73). С. 143–148.

36. Новокшонов А. К. Захищені групові комунікації: особливості програмної реалізації. Вісник Київського національного університету імені Тараса Шевченка. Серія "Фізико-математичні науки". 2015. Вип. № 1. С. 159–162.

37. Остапов С. Е., Євсєєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту. Львів: Новий світ - 2000, 2020. 678 с.

38. Остроухов В. В., Присяжнюк М. М. Інформаційна безпека: Підручник. Київ: Ліра-К, 2021. 412 с.

39. Парасій-Вергуненко І. М. Методика аналізу клієнтської бази банку. Фінанси України. 2005. № 10. С. 68–75.

40. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: ювілейна наук.-техн. конференція, Київ 9-11 червня 1998: Присвяч. 100-ю КПІ та 5-ю Держ. ком. України з питань держ. секретів та тех. зах. інформації. Київ, 1998. 280 с.

41. Пучков О.О. Нормативні засади правопорядку у сфері національної безпеки України. 2016.

42. Ришковський П. М. Засоби збору і передачі інформації. Львів, 1977. 128 с.

43. Рубанов В. В. "Політична аналітика": досвід та перспективи експлікації поняття. Гілея. 2012. Вип. 57 (№ 2). С. 581–583.

44. Світвуд А. Маркетингова аналітика. Як підкріпити інтуїцію даними. Львів: Наш Формат, 2019. 152 с.

45. Скабцов М. Аудит безпеки інформаційних систем. 2018: Пітер Прес, 2018. 272 с.

46. Сорос Дж. Відкрите суспільство. Реформування глобального капіталізму. 2-ге вид. Львів: Фоліо, 2018. 364 с.

47. Сорос Дж. На захист відкритого суспільства. Львів: Vivat, 2021. 224 с.

48. Тимошенко Є. М. Технічний захист інформації на підприємстві: Thesis. 2021. URL: http://ir.stu.cn.ua/123456789/24855.

49. Тунік А. Персональні дані, інформація про особу, конфіденційна інформація про особу: аспекти співвідношення. Підприємництво, господарство і право. 2012. № 5 (197). С. 50–54.

50. Філіпова Л. Я. Автоматизовані бази даних у світовому інформаційному просторі. Вісник Харківської державної академії культури. 1999. Вип. 1. С. 144–152.

51. Data-Driven Analytics for Personalized Medical Decision Making / N. Melnykova et al. Mathematics. 2020. Vol. 8, no. 8. P. 1211. URL: https://doi.org/10.3390/math8081211.

52. Маковець С. Внутрішній ворог. Де найслабша ланка при кібератаках? Блог Сергія Маковця [Електронний ресурс] / Сергій Маковець // Новини науки і техніки. IT, винаходи та розробки - НВ Техно. Режим доступу: https://techno.nv.ua/ukr/technoblogs/vnutrishnij-vorog-de-najslabsha-lanka-pri-kiberatakah-blog-sergija-makovtsja-2088833.html (дата звернення: 12.03.2024).

53. Помста звільнених працівників: як вони шкодять інформаційної безпеки компаній? // http://www.trud.gov.ua/control/uk/publish/article?art_id=512093.

54. Група компаній «ФОКСТРОТ»: «фокстрот. техніка для дома», foxmart, техношара, секунда, depot center, fantasy town [Електронний ресурс] // Група компаній «ФОКСТРОТ». Режим доступу: https://foxtrotgroup.com.ua/ (дата звернення: 08.04.2024).

55. Ivanti - автоматизація IT-операцій і операцій із забезпечення захисту [Електронний ресурс] // ESKA. Режим доступу: https://eska.global/products/ivanti (дата звернення: 17.05.2024).

56. Ivanti - Everywhere Work. Elevated. [Електронний ресурс]. Режим доступу: https://www.ivanti.com/ (дата звернення: 17.05.2024).

ДОДАТКИ

ДОДАТОК А

Таблиця 1.1. Ризики та загрози аналітичної культури

Ризики	**Загрози, які вони несуть**
Відсутність якості даних	Недостатні або низькоякісні дані можуть підірвати цілісність і точність аналітичних висновків. Цей ризик може виникати через помилки збору даних, неповні або суперечливі дані або неадекватні процеси перевірки даних. Це може призвести до помилкових аналізів і оманливих висновків.
Упереджені дані	Упереджені дані, що надходять із різноманітних джерел, як-от упередження вибірки чи методи збору даних, можуть призвести до викривлення аналітичних результатів. Якщо дані, використані в аналізі, не є репрезентативними або містять властиві упередження, це може призвести до неправильних припущень і дискримінаційних результатів.
Невідповідна конфіденційність і безпека даних	Недостатні заходи щодо захисту конфіденційності та безпеки даних можуть призвести до несанкціонованого доступу, витоку даних або неправомірного використання конфіденційної інформації. Втрата або компрометація даних може мати серйозні наслідки, включаючи шкоду репутації, юридичні наслідки та порушення правил конфіденційності.
Неправильне тлумачення аналітичного результату	Аналітичні висновки можуть бути неправильно витлумачені через брак розуміння чи досвіду. Коли люди неправильно тлумачать або неправильно застосовують аналітичні результати, це може призвести до неправильного прийняття рішень і дій на основі помилкових припущень або неправильної інтерпретації даних.
Відсутність прозорості в аналізі	Відсутність прозорості в аналітичних процесах, методології та припущеннях може підірвати довіру та надійність. Коли зацікавлені сторони не можуть оцінити валідність і

	надійність аналітичних результатів, досягти консенсусу та прийняти обґрунтовані рішення на основі аналізу стає складно.
Погане управління даними	Погана практика управління даними, неадекватна документація та відсутність обслуговування даних можуть призвести до неправильного управління даними. Це включає такі проблеми, як дублювання даних, втрата даних, неправильне зв’язування даних і застарілі дані, які можуть призвести до помилкових аналітичних результатів і ненадійної інформації.
Відсутність аналітичних навичок	Недостатні навички та знання методів аналізу даних, статистичного моделювання та інтерпретації результатів можуть обмежити ефективність аналітичної культури. Без міцної основи аналітичних навичок організаціям може бути важко використовувати дані для прийняття обґрунтованих рішень.
Опір змінам	Опір прийняттю в організації аналітичного підходу, який базується на даних, може перешкодити розвитку аналітичної культури. Відсутність підтримки, небажання приймати нові методології та опір змінам можуть перешкоджати прогресу та обмежувати переваги, які може запропонувати аналітика.
Технічні обмеження	Технічні обмеження, такі як невідповідна інфраструктура, застарілі програмні засоби або недостатня обчислювальна потужність, можуть перешкоджати реалізації та ефективності аналітичних процесів. Ці обмеження можуть обмежувати масштаб, швидкість і складність аналізу, впливаючи на якість отриманої інформації.

ДОДАТОК Б

Інтерв'ю з Олексієм Пащенком, керівником відділу служби інформаційної безпеки групи компаній «Фокстрот»

Як називається організація, відповідальна за захист інформації, і яка її організаційна структура? Хто виконує ключові ролі та відповідальність у забезпеченні інформаційної безпеки?

Олексій: Відділ інформаційної безпеки знаходиться в штаті управляючої компанії Групи компаній «Фокстрот». Наразі у відділі працюють два працівника – керівник відділу (тобто я) та менеджер із захисту інформації. Всі функції та процеси, пов'язані з інформаційною безпекою, розподілені між нами.

Яка загальна ціль або завдання інформаційної безпеки в організації? Як компанія визначає пріоритет захисту конфіденційної інформації?

Олексій: Головна мета – забезпечення безпеки інформаційних активів Групи компаній «Фокстрот» та безперервності діяльності бізнесу за рахунок впровадження системи управління інформаційною безпекою (СУІБ), грамотної експлуатації засобів захисту інформації (ЗЗІ) та адекватного реагування на інциденти інформаційної безпеки.

Яких стандартів Міжнародної організації зі стандартизації (ISO) компанія дотримується у своїй практиці захисту інформації?

Олексій: Ми намагаємося дотримуватись у роботі вимог серії стандартів ISO/IEC 27000. Прямих вимог щодо обов'язкового дотримання стандартів у нашій галузі наразі немає, але ми орієнтуємося на ці стандарти як на кращі практики.

Як компанія здійснює моніторинг та аналіз потенційних загроз інформаційній безпеці? Які інструменти, технології чи процеси існують для виявлення інцидентів або порушень безпеки та реагування на них?

Олексій: Ми впровадили комплексний набір систем захисту для виявлення, аналізу та блокування загроз. Серед основних систем: Next Generation Firewall, корпоративна система Endpoint Detection and Response, Email Security Appliance, Web Application Firewall, система управління вразливостями (сканер вразливостей), SIEM-система, DLP-система. Моніторинг подій інформаційної безпеки в IT-інфраструктурі делеговано на аутсорсинг комерційному Security Operation Center (SOC).

Як проводяться регулярні аудити для оцінки стану безпеки в інформаційних системах організації? Ці аудити проводяться внутрішніми аудиторами чи зовнішніми сторонніми аудиторами? Яких методологій чи рамок дотримуються під час аудитів?

Олексій: Проводяться періодичні зовнішні загальні аудити безпеки (регламент не встановлено). Внутрішні аудити проводяться внутрішнім відділом інформаційної безпеки в рамках робочих процесів.

Які заходи існують для забезпечення фізичної безпеки конфіденційної інформації? Як реалізуються та контролюються засоби контролю доступу, відеоспостереження та інші заходи фізичної безпеки?

Олексій: Фізична безпека знаходиться в компетенції служби безпеки. Інформаційна безпека адмініструє систему контролю доступу, яка включає адміністрування доступу до режимних приміщень, таких як серверні та комутаційні приміщення.

Як компанія забезпечує доступ і автентифікацію користувачів? Які механізми використовуються для перевірки особи та авторизації осіб, які мають доступ до конфіденційної інформації чи систем?

Олексій: У нас розгорнута служба Windows Active Directory, яка забезпечує автентифікацію користувачів у більшості корпоративних додатків та систем. В системах з підвищеним рівнем критичності або для облікових записів з привілейованими правами використовується багатофакторна автентифікація (MFA).

Чи існують спеціальні політики та процедури щодо класифікації, обробки та утилізації конфіденційної інформації? Як забезпечується захист даних протягом життєвого циклу інформації?

Олексій: Так, у нас є набір внутрішніх політик та процедур, пов'язаних з інформаційною безпекою. Наприклад, політика інформаційної безпеки Групи компаній «Фокстрот», положення про оцінювання та класифікацію інформації, положення про управління інформаційними активами.

Чи проводить компанія регулярні тренінги та програми підвищення обізнаності для працівників щодо найкращих практик інформаційної безпеки? Як працівники ознайомлені з їхніми ролями та обов'язками щодо захисту конфіденційних даних?

Олексій: Так, у нас проводяться періодичні розсилки для інформування та нагадування працівникам про основні вимоги інформаційної безпеки. Вимоги щодо норм інформаційної безпеки доводяться до працівників окремо через керівників.

Як компанія реагує на інциденти та порушення? Що таке план реагування на інцидент і хто відповідає за його координацію та виконання? Чи є задокументовані приклади дій з реагування на інциденти, вжитих у минулому?

Олексій: У нас розроблені правила реагування на типові події інформаційної безпеки, які виявляються за допомогою Security Operation Center. За координацію дій та виконання таких правил відповідає відділ інформаційної безпеки. Нетипові інциденти вимагають проведення додаткового розслідування з залученням необхідних співробітників з різних підрозділів, таких як служба безпеки та юридичний департамент.

Як компанія забезпечує безпеку інформації, коли вона передається або надається зовнішнім особам, таким як постачальники, партнери чи клієнти? Чи існують безпечні протоколи зв'язку чи механізми шифрування?

Олексій: Стандартизованого механізму захищеної передачі інформації третім особам не встановлено. Методи та вимоги можуть формуватися окремо

для різних випадків в залежності від бізнес-процесу або критичності інформації, яку потрібно передавати.

Які стратегії резервного копіювання та аварійного відновлення використовуються для захисту від втрати даних і забезпечення безперервності бізнесу в разі інциденту безпеки або збою системи?

Олексій: Ми розробляємо, впроваджуємо та тестуємо плани забезпечення безперервності бізнесу (BCP) та плани аварійного відновлення (DRP), які визначають порядок та послідовність дій у разі виникнення інциденту, що потребує активації плану. Відповідальним за розроблення та тестування планів є наш відділ інформаційної безпеки.

Чи є спеціальна команда або відділ, відповідальний за інформаційну безпеку в організації? Як розподіляються обов'язки з безпеки між різними групами чи відділами?

Олексій: Так, у нас є відділ інформаційної безпеки, який відповідає за всі процеси, пов'язані з інформаційною безпекою в групі компаній. Основні функції нашого відділу включають організацію та координацію робіт, впровадження та експлуатацію засобів захисту інформації, дослідження технологій обробки інформації з метою виявлення можливих загроз, інвентаризацію інформаційних активів, впровадження та підтримку систем моніторингу, розробку нормативних документів, планування та організацію робіт із залученням підрядних організацій, тестування безпеки програмних комплексів, підвищення обізнаності працівників, участь у розслідуванні інцидентів.

ДОДАТОК В

Попередження співробітників ГК «Фокстрот» про масову розсилку фішингових листів

This message was sent with High importance.

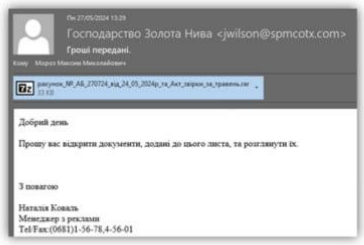
Support<SupportAll@foxtrot.ua>

Reply | Reply all | Forward

Tue 5/28/2024 11:10 AM

Шановні співробітники!

Останніми днями фіксується збільшення кількості масових розсилок шкідливих електронних листів, що вказує на чергову спрямовану кібератаку на нашу групу компаній. Зловмисники надсилають листи, у яких вкладений архів з файлами, що містять шкідливий програмний код. Зазвичай такий архів має назву: "Рахунок_№_АБ_270724_від_24_05_2024р_та_Акт_звірки_за_травень.rar"
Приклад такого листа:



Теми листів різняться, але містять фінансову складову та закликають звернути на них увагу, наприклад: "Гроші відправлено.", "Гроші передані.", "Розрахунок переданий.", "Оплата виконана.", "Платіж виконаний.", "Платіж надіслано." тощо. Ці листи приходять від різних відправників і можуть здатися офіційними, відправляються не автоматизованими методами, тому засоби захисту поштової системи не завжди здатні відрізнити такі листи від звичайної кореспонденції і можуть доставити їх користувачу.
Відкриття вкладених файлів призводить до зараження операційної системи і надає зловмисникам можливість віддалено керувати зараженим пристроєм.

Будьте пильні!

Щоб уберегтись від наслідків атаки слід запам'ятати просте правило: **не відкривайте підозрілі файли, посилання, вкладення електронної пошти, або архіви, якщо ви не довіряєте відправнику.** Файли або посилання від людей, яких ви не знаєте, повинні розцінюватися як шкідливі за замовчуванням.

Якщо у вас є сумніви щодо надійності вхідного листа, перешліть його на перевірку на адресу SupportAll@foxtrot.ua

E-mail SupportAll@foxtrot.ua
Внутрішній тел **911**
Корп. мобільний **(066) 8-777-911**
Міський номер **(044) - 537-48-48**
Telegram Viber WebSD

Reply | Reply all | Forward

ДОДАТОК Г

Відгук працівника ІТ-департаменту на план-проєкт впровадження рішень Ivanty у роботу ГК «Фокстрот»

Поліна Андріївна Фрідріх <polina.fridrikh@oa.edu.ua>

План впровадження
Повідомлень: 2

Поліна Андріївна Фрідріх <polina.fridrikh@oa.edu.ua> 12 квітня 2024 р. о 09:40
Кому: robenko-o@foxteam.digital

Шановний пане Олександр,

Мене звати Поліна, я студентка Національного університету "Острозька академія". Надсилаю вам план впровадження системи Ivanti для вашої компанії, в якому розглянуто поточний стан ваших інформаційних систем, визначено вимоги до нової системи, а також розроблено детальний план тренування персоналу. У плані враховано аналіз можливих ризиків, стратегії для їх управління, та економічну оцінку вартості впровадження.

Буду вдячна за ваші коментарі та зворотний зв'язок, що допоможе вдосконалити мої навички та врахувати ваші рекомендації для подальших проектів.

З повагою, Поліна, студентка Національного університету "Острозька академія"

План впровадження.xlsx
16K

Робенко Олександр Олександрович <Robenko-O@foxteam.digital> 12 квітня 2024 р. о 13:44
Кому: Поліна Андріївна Фрідріх <polina.fridrikh@oa.edu.ua>

Шановна пані Поліно,

Дякую за ваш план впровадження системи Ivanti. Він показує глибоке розуміння технічних та організаційних аспектів. Особливо відзначаю чітку структуру плану, який охоплює всі етапи впровадження, оцінку ризиків і стратегії управління ними, тренування персоналу та адаптацію системи під потреби нашої компанії, а також обґрунтовані розрахунки вартості та вигод.

Для подальшого покращення плану рекомендую додати більше деталей про інтеграцію Ivanti з існуючими системами, провести аналіз очікуваних покращень продуктивності, а також розробити механізми отримання зворотного зв'язку від користувачів на кожному етапі впровадження.

Ваш план є високоякісним і обґрунтованим. Впевнений, що його реалізація покращить роботу нашої компанії. Дякую за вашу роботу і бажаю успіхів у подальших дослідженнях.

З повагою,
Олександр РОБЕНКО
Адміністратор компанії Foxteam Digital