МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально–науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В.Легомінова
«___»_____20__ р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В.Легомінова
«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

МЕТОДИ ТА ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВНУТРІШНІХ ЗАГРОЗ НА ПІДПРИЄМСТВІ

СТУДЕНТ**:** Стародубець Владислав Олександрович _____
(підпис)

НАУКОВИЙ КЕРІВНИК: к.т.н. Рабчун Дмитро Ігорович _____
(підпис)

НОРМОКОНТРОЛЕР: к.т.н., доц. Дзюба Тарас Михайлович _____
(підпис)

Київ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри УІКБ

_____ С.В.Легомінова

(підпис)

«___» _____ 20__ р.

ЗАВДАННЯ

на дипломну роботу

студенту Стародубцю Владиславу Олександровичу

1. Тема роботи «Методи та організація захисту інформації від внутрішніх загроз на підприємстві», затверджена наказом по університету № 170 від «11» жовтня 2021 р.

2. Термін здачі студентом оформленої роботи «24» грудня 2021 р.

3. Об'єкт дослідження: процеси забезпечення інформаційної безпеки підприємства.

4. Предмет дослідження: методи захисту данних від внутрішніх загроз.

5. Мета дослідження: визначити шляхи вдосконалення процесів протистояння витокам інформації із внутрішніх активів підприємства.

6. Перелік питань, які мають бути розроблені:

1. Вивчення основних характеристик внутрішніх загроз на підприємстві.
2. Дослідження методів та інструментів для організації захисту від внутрішніх загроз на підприємстві.
3. Визначення рекомендацій щодо організації захисту інформаційних активів від внутрішніх загроз.

7. Дата видачі завдання «16» вересня 2021 р.

Науковий керівник _____ Д.І. Рабчун

підпис

Завдання прийнято до виконання _____ В.О. Стародубець

підпис

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

студентом Стародубцем Владиславом Олександровичем

Дата видачі завдання: «16» вересня 2021 р.

№ з/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	16.09.2021	
2.	Збір та аналіз літератури.	28.09.2021	
3.	Вивчення основних характеристик внутрішніх загроз на підприємстві.	12.10.2021	
4.	Дослідження методів та інструментів для організації захисту від внутрішніх загроз на підприємстві.	26.10.2021	
5.	Визначення рекомендацій щодо організації захисту інформаційних активів від внутрішніх загроз.	09.11.2021	
6.	Формулювання висновків за результатами проведеного дослідження.	23.11.2021	
7.	Оформлення роботи.	07.12.2021	
8.	Оформлення презентації.	14.12.2021	
9.	Отримання рецензії на роботу.	24.12.2021	
10.	Захист в ДЕК.	18.01.2022	

Студент: Стародубець Владислав Олександрович _____

(підпис)

Науковий керівник: Рабчун Дмитро Ігорович _____

(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню методів та організації захисту інформації від внутрішніх загроз на підприємстві. Робота складається зі вступу, трьох розділів, що містять 17 рисунків та 1 таблицю, висновків до кожного розділу, загальних висновків, списку використаних джерел із 62 найменувань. Загальний обсяг роботи становить 84 аркуша, з яких 6 аркуші займає список використаних джерел.

Об'єкт дослідження – процеси забезпечення інформаційної безпеки підприємства.

Предмет дослідження – методи захисту даних від внутрішніх загроз.

Мета дослідження – визначити шляхи вдосконалення процесів протистояння витокам інформації із внутрішніх активів підприємства.

У дипломній роботі на основі вивчення та аналізу відповідних джерел визначимо основні особливості внутрішніх порушень інформаційній безпеці підприємства, розглянемо типову модель порушника та класифікуємо «невдоволених» співробітників, дослідимо вектор розвитку внутрішніх атак й тенденції з кібербезпеки в різних країнах світу та запропонуємо основні методи та інструменти захисту для збереження конфіденційних та персональних даних усередині підприємства.

Сфера застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи захисту інформаційних активів підприємства у контексті протидії внутрішнім загрозам, пов'язаним із витоками конфіденційних даних.

Ключові слова: ВНУТРІШНІ ЗАГРОЗИ, ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, МОДЕЛЬ ПОРУШНИКА, ДЖЕРЕЛА ЗАГРОЗ, ІНФОРМАЦІЙНІ АКТИВИ, КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ.

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність і своєчасність звернення до даного питання обумовлена тим, що, на сьогодні найбільшу загрозу інформаційній безпеці представляють внутрішні зловмисники. З кожним роком ця загроза все зростає. Часи, коли керівники підприємств боялися атак хакерів і вірусів тепер в минулому. Звичайно, даний клас загроз донині несе в собі велику небезпеку, але найбільше компанії стурбовані саме через втрату й виток корпоративної інформації й персональних даних. Про це говорять результати практично будь-яких досліджень в області інформаційної безпеки.

«Нехороші» співробітники своїми нелегітимними діями всередині підприємства можуть завдати йому шкоди не тільки у вигляді витоків даних, але й у вигляді прямої крадіжки грошових і матеріальних ресурсів з використанням IT-систем. Бувають випадки, коли персонал організовує реальні хакерські атаки всередині компанії. Наприклад, дуже складно протистояти загрозам, при реалізації яких співробітники компанії вступають в змову з третіми особами. Так, якщо зловмисникові вкрай непросто впровадити шкідливий код в продакшн-систему (для цього потрібно обійти масу бар'єрів і тільки після цього провести впровадження коду, який буде, наприклад, перенаправляти зловмисникові інформацію про замовлення в інтернет-магазині), то при можливості «домовитися» з розробником програми завдання істотно спрощується. [1]

За деякими оцінками, внутрішній співробітник сьогодні виявляється замішаний в 80% Кібер-інцидентів. Зловмисники спочатку захоплюють ідентифікаційні дані внутрішнього співробітника і вже потім діють від його імені.

Дослідження інституту SANS показали, що 74% опитаних ІБ-фахівців стурбовані внутрішніми загрозами; 32% визнають, що у них немає можливостей протистояти інсайдерам, 28% відзначили, що в їхніх організаціях захист від інсайдерів взагалі не вважається пріоритетною; 62% вважають, що в планах

реагування на інциденти немає відмінності між зовнішніми нападниками та внутрішніми.

Водночас в нещодавно опублікованих компанією Solar Security результатах досліджень приблизно 64% вивчених її фахівцями ІБ-інцидентів, були класифіковані як такі, що мали внутрішні причини. [2]

Внутрішні атаки залишаються найнебезпечнішими через розміри заподіюваних ними прямих збитків. Це підтверджують щорічні звіти, що публікуються ISACA, PwC, Verizon і іншими аналітичними компаніями. Відбувається це тому, що потенційний внутрішній порушник знає, як влаштовані інформаційні системи, і часто у своєму розпорядженні має прямий доступ до конфіденційної інформації. Крім того, внутрішньому порушнику заздалегідь відомо, яку інформацію можна використовувати для вилучення особистої вигоди.

Для протидії внутрішнім загрозам застосовують спеціалізовані засоби захисту та комплексні рішення, спрямованими на протидію таргетованим атакам: пісочниці, системи управління ІБ і подіями ІБ, веб-шлюзи, шлюзи електронної пошти, засоби моніторингу дій адміністраторів та інших привілейованих користувачів, контроль виконуваних транзакцій і поведінкових моделей, контроль вразливостей інфраструктурних компонентів і бізнес-додатків й ін.

Комплексний підхід до захисту в першу чергу виражається в кореляції подій безпеки та інтеграції різних механізмів захисту між собою. Сучасна система захисту повинна будуватися не на розрізнених засобах захисту, здатних працювати тільки у своїй вузькій сфері, а на комплексних продуктах, які вміють зіставляти між собою різні події та дозволяють виробляти комплексну реакцію в залежності від загальної ситуації.

Не можна також забувати, що забезпечення ІБ - безперервний процес. Поки існує сама інформація, що вимагає захисту, система менеджменту ІБ (СМІБ) повинна ґрунтуватися на відомій моделі PDCA (Plan-Do-Act-Control, плануй - роби - перевіряй - впливай).[3]

Таким чином, на основі вивчення та аналізу відповідних джерел визначимо основні особливості внутрішніх порушень інформаційній безпеці підприємства, розлянемо типову модель порушника та класифікуємо «невдоволених» співробітників, дослідимо вектор розвитку внутрішніх атак й тенденції з кібербезпеки в різних країнах світу та запропонуємо основні методи та інструменти захисту для збереження конфіденційних та персональних даних усередині підприємства.

Мета і завдання дослідження. **Мета роботи** визначити шляхи вдосконалення процесів протистояння витокам інфорамції із внутрішніх активів підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Вивчення основних характеристик внутрішніх загроз на підприємстві.
2. Дослідження методів та інструментів для організації захисту від внутрішніх загроз на підприємстві.
3. Визначення рекомендацій щодо організації захисту інформаційних активів від внутрішніх загроз.

Об’єкт дослідження – процеси забезпечення інформаційної безпеки підприємства.

Предмет дослідження – методи захисту данних від внутрішніх загроз.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи теоретичного аналізу літератури, методи аналізу, синтезу та порівняння, соціологічні методи.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації комплексу заходів з захисту активів підприємства від внутрішніх загроз.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу контролювати дії користувачів та працівників підприємства, захистити конфіденційні дані в інформаційній системі підприємства.

РОЗДІЛ 1
ОСНОВНІ ХАРАКТЕРИСТИКИ ВНУТРІШНІХ ЗАГРОЗ НА ПІДПРИЄМСТВІ

1.1. Внутрішні загрози на підприємстві

Під внутрішніми загрозами інформаційної безпеки розуміються загрози з боку співробітників компанії як навмисні (шахрайство, крадіжка, спотворення чи знищення конфіденційної інформації, промислове шпигунство тощо), так і ненавмисні (зміна або знищення інформації через низьку кваліфікацію співробітників або неуважність), а також збої програмних чи апаратних засобів обробки та зберігання інформації.

Всі загрози інформаційної безпеки поділяються на зовнішні та внутрішні. Існує думка, що, захистившись від зовнішніх загроз (хакерських атак і зломів), завдання інформаційної безпеки вирішені. Це не так: численні інциденти і досвід показують, що небезпечніші внутрішні загрози.

Минулого року понад 60% вітчизняних компаній зіткнулися з витоком інформації, як свідчать дані дослідження «SearchInform». Але серед основних загроз інформаційній безпеці не лише витоки, а й непродуктивність та шахрайство з боку співробітників, корпоративне шпигунство та просте злодійство. У міру переходу бізнесу до цифри ризик перелічених загроз зростає, і компанії збільшують бюджети на інформаційну безпеку.

Традиційне питання про витік показує, що ситуація з ними залишається стабільною: кількість компаній, які фіксували такі інциденти, щороку впевнено перевалює за половину. Але це зовсім не означає, що у компаній, що залишилися (у 2020 році таких 34%) зовсім не було витоків. Витоки могли бути просто не виявлені.

При цьому для бізнесу набагато важливіше інциденти, які несуть прямі фінансові збитки. Так, 41,5% респондентів зіткнулися з використанням ресурсів

компанії в особистих цілях, 21% - зі спробою відкатів, 18,5% - з промисловим шпигунством.

Рис 1.1. Використання ресурсів підприємства

Внутрішні загрози - це загрози, які пов'язані зі співробітниками організації, тобто людським фактором. Можна виділити наступні основні види внутрішніх загроз:

- **навмисні або ненавмисні дії співробітника підприємства, які призвели до пошкодження / видалення інформації.** У разі нормальної роботи відділу інформаційних технологій та інформаційної безпеки такі інциденти не повинні призводити до фатальних наслідків - інформація просто відновлюється з резервної копії;
- **навмисні або ненавмисні дії співробітника підприємства, які призвели до витоку конфіденційної інформації за межі підприємства.** Це серйозний інцидент безпеки, який можна запобігти, якщо система інформаційної безпеки на підприємстві вибудувана відповідно до кращих практик та рекомендацій по ІБ;
- **фізичне руйнування (навмисне або ненавмисне) систем безпеки або інформаційних систем співробітниками підприємства.** Даний інцидент безпеки зустрічається рідко, і призводить до серйозного матеріального збитку - тут вже мова йде про норми кримінального кодексу, а це - сфера діяльності

правоохоронних органів. Єдиний спосіб уникнути цієї загрози - взаємодія зі службою фізичної безпеки та охорони підприємства, тобто впровадження системи контролю управління доступом в приміщення (СКУД) і системи відеоспостереження;

- **дії співробітника (або групи співробітників), що здійснюються з використанням соціальної інженерії і психологічних маніпуляцій**. Особливість такого інциденту в тому, що дуже часто співробітники навіть не припускають, що ними маніпулюють, а ініціатор дій може перебувати поза межами підприємства, іноді навіть в іншій країні. Запобігання інцидентів цього виду можливо тільки одним способом - аналізом комунікацій співробітників, що робиться за допомогою спеціалізованого програмного забезпечення.

У 74% випадків інциденти допускали пересічні працівники. Лідерами за кількістю порушень стали менеджери відділу постачання: вони були причетні до 25,5% інцидентів. На другому місці бухгалтери, економісти та фінансисти (24%), за ними йдуть помічники керівника (16,2%) та IT-фахівці (14,8%). Звичайно, ці цифри має сенс розглядати з поправкою: служби безпеки традиційно контролюють працівників на корупційно містких посадах: бухгалтерів, фінансистів — там, де втрати можуть бути серйознішими. У компанії з 2000 співробітників служба безпеки може контролювати невелику групу ризику з 20 осіб, решту інших ігнорувати, припускаючи, що за ними повинні доглядати лінійні керівники. Така позиція має право на життя, якщо служба безпеки розуміє та приймає можливі ризики.

Рис 1.2. Працівники по посадах

Прямі чи непрямі втрати зазнали 83% компаній, що зіткнулися з Кібер-інцидентами. Це призвело до іміджевих і дрібних фінансових збитків (28%), а також до великих фінансових збитків (13%) і compliance-ризиків — загрози або факту покарання від регулятора (12%).

Рис 1.3. Втрати пов'язані з Кібер-інцидентами

Внутрішні атаки залишаються найнебезпечнішими через розміри заподіюваних ними прямих збитків. Це підтверджують щорічні звіти, що публікуються ISACA, PwC, Verizon і іншими аналітичними компаніями.

Відбувається це тому, що потенційний внутрішній порушник знає, як влаштовані інформаційні системи, і часто у своєму розпорядженні має прямий доступ до конфіденційної інформації. Крім того, внутрішньому порушнику заздалегідь відомо, яку інформацію можна використовувати для вилучення особистої вигоди. [4]

1.2. Модель внутрішнього порушника

Модель порушника - абстрактний (формалізований або неформалізований) опис порушника правил розмежування доступу.

Модель порушника визначає:

- категорії (типи) порушників, які можуть вплинути на об'єкт;
- цілі, які можуть переслідувати порушники кожної категорії, можливий кількісний склад, інструменти, приладдя, оснащення, зброю та ін.;
- типові сценарії можливих дій порушників, що описують послідовність (алгоритм) дій груп та окремих порушників, способи їх дій на кожному етапі.

Модель порушників може мати різний ступінь деталізації.

- Змістовна модель порушників відображає систему прийнятих керівництвом об'єкта, відомства поглядів на контингент потенційних порушників, причини та мотивацію їх дій, цілі, що переслідуються, і загальний характер дій у процесі підготовки та здійснення акцій впливу.
- Сценарії впливу порушників визначають класифіковані типи вчинених порушниками акцій з конкретизацією алгоритмів та етапів, а також способів дії на кожному етапі.
- Математична модель впливу порушників являє собою формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушників, кількісних значень, що параметрично характеризують результати дій, і функціональних (аналітичних, чисельних або алгоритмічних) залежностей, що описують процеси взаємодії порушників, що протікають, з елементами

об'єкта і системи охорони. Саме цей вид моделі використовується для кількісних оцінок вразливості об'єкта та ефективності охорони.

Внутрішній порушник

Під внутрішнім порушником розуміють порушника, що усередині інформаційної системи на момент початку реалізації загрози.

Спробуємо спочатку класифікувати «невдоволених» співробітників:

- Ті, хто вважає, що їм не доплачують.
- Ті, хто вважає, що має обіймати вищу посаду.
- Ті, хто вважає, що його не поважають особисто або не зважають на його думку.
- Ті, хто заздрить добробуту роботодавця.
- Ті, хто просто звикли за властивостями свого характеру шкодити, де це можливо.
- Ті, хто незадоволений роботою в компанії з якоїсь іншої причини.
- Ті, хто зібрався звільнитися.

Правильно розроблена модель порушника є гарантією побудови адекватної системи забезпечення інформаційної безпеки. Маючи побудовану модель, вже можна будувати адекватну систему інформаційного захисту.

Найчастіше будується неформальна модель порушника, що відображає причини й мотиви дій, його можливості, апріорні знання, цілі, їх пріоритетність для порушника, основні шляхи досягнення поставлених цілей: способи реалізації вихідних від нього загроз, місце і характер дії, можлива тактика і т.д. Для досягнення поставленої мети порушник повинен докласти певних зусиль і витратити деякі ресурси.

Визначивши основні причини порушень, є можливим вплинути на них або необхідним чином скоригувати вимоги до системи захисту від такого типу загроз. Під час аналізу порушень захисту необхідно приділяти увагу суб'єкту (особистості) порушника. Усунення причин або мотивів, що спонукали до порушення, може допомогти уникнути повторення подібного випадку.

Модель може бути не одна, доцільно побудувати кілька різних моделей різних типів порушників інформаційної безпеки об'єкта захисту.

Для побудови моделі порушника використовується інформація, отримана від служб безпеки та аналітичних груп, дані про наявні засоби доступу до інформації та її обробки, про можливі способи перехоплення даних на стадіях їх передачі, обробки та зберігання, про обстановку в колективі та на об'єкті захисту, відомості про конкурентів і ситуацію на ринку, відбулися випадки порушення інформаційної безпеки тощо.

Крім цього оцінюються реальні оперативні технічні можливості зловмисника для впливу на систему захисту або на об'єкт, що захищається. Під технічними можливостями мається на увазі перелік різних технічних засобів, які може мати порушник у процесі здійснення дій, спрямованих проти системи інформаційного захисту.

Можливості внутрішнього порушника істотно залежать від наявних в межах контрольованої зони обмежувальних факторів, з яких основним є реалізація комплексу режимних та організаційно-технічних заходів, в тому числі по підбору, розставлювання та забезпечення високої професійної підготовки кадрів, допуску фізичних осіб всередину контрольованої зони й контролю за порядком проведення робіт, спрямованих на запобігання і припинення несанкціонованих дій.

Виходячи з особливостей функціонування АС, допущені до неї фізичні особи, мають різні повноваження на доступ до інформаційних, програмних, апаратних та інших ресурсів відповідно до прийнятої політики інформаційної безпеки (правилами). До внутрішніх порушників можуть належати:

- адміністратори АС (категорія I);
- технічний персонал АС (співробітники експлуатаційних підрозділів, що здійснюють технічний супровід обладнання, програмного забезпечення і засобів захисту інформації) (категорія II);
- користувачі АС (категорія III);

- співробітники, що мають санкціонований доступ в службових цілях в приміщення, в яких розміщуються активи АС, але не мають права доступу до активів (категорія V);
- обслуговуючий персонал (охорона, працівники інженерно технічних служб і т.д.) (категорія VI);
- уповноважений персонал розробників АС, який на договірній основі має право на технічне обслуговування і модифікацію компонентів АС (категорія VII).

На осіб категорії I та II покладені завдання по адмініструванню і технічного супроводу програмно-апаратних засобів АС. Адміністратори й технічний персонал АС потенційно можуть проводити атаки, використовуючи можливості по безпосередньому доступу до інформації, що захищається, що обробляється і зберігається в АС, а також до технічних і програмних засобів АС, включаючи засоби захисту, які використовуються в АС, відповідно до встановлених для них адміністративними повноваженнями.

Ці особи добре знайомі з основними алгоритмами, протоколами, реалізованими та використовуваними в АС, а також з наявними принципами й концепціями безпеки.

Передбачається, що вони могли б використовувати стандартне обладнання або для ідентифікації вразливостей, або для проведення атак. Дане обладнання може бути як частиною штатних засобів, так і може ставитися до легко отримується (наприклад, програмне забезпечення, отримане з загальнодоступних зовнішніх джерел).

Крім того, передбачається, що ці особи могли б мати у своєму розпорядженні спеціалізоване обладнання.

Для забезпечення захисту від внутрішніх порушників у трудових угодах із працівниками компанії прописують пункти про відповідальність за розголошення конфіденційної інформації, а також запроваджують режим комерційної таємниці, який, відповідно до законодавства, дозволяє захистити інтереси роботодавця. [5]

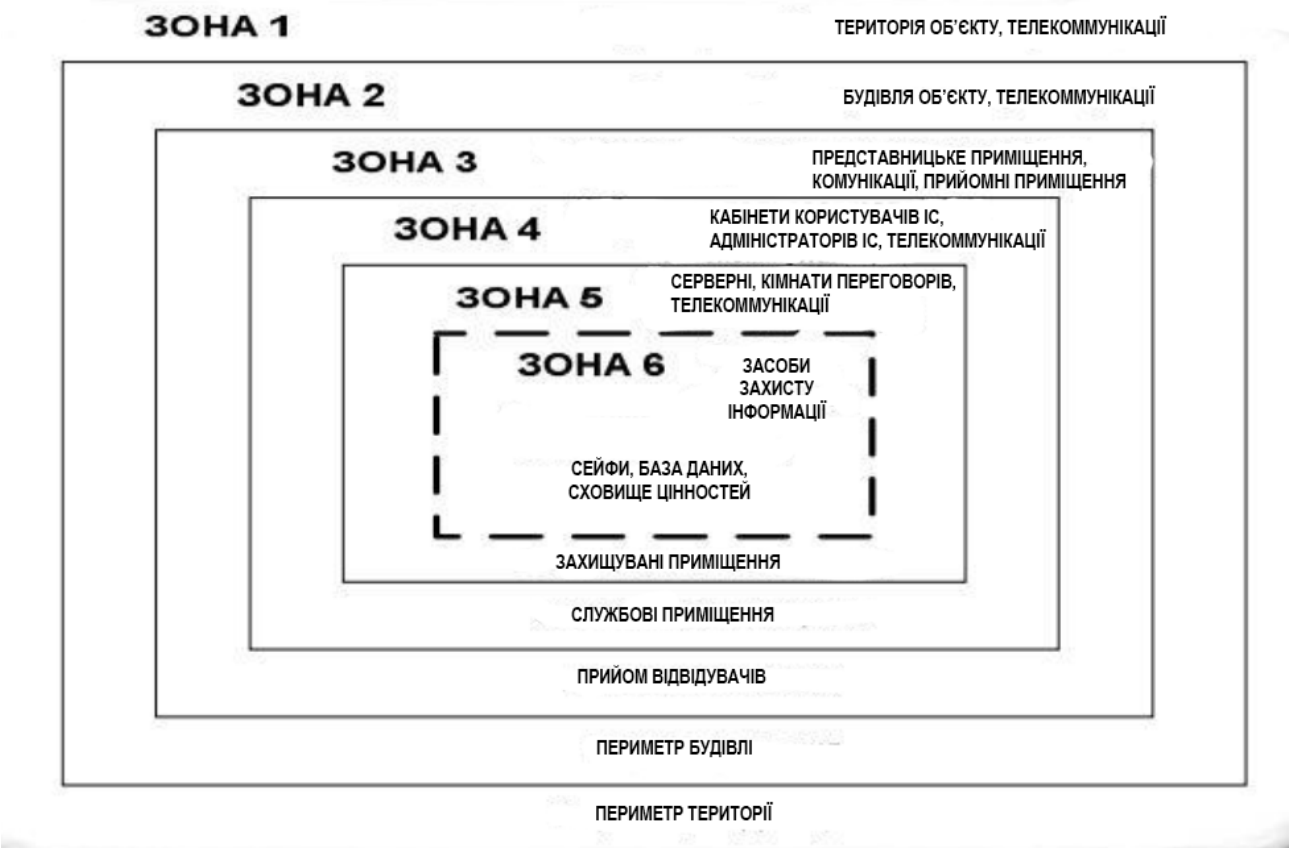

Рис .1.4. Рубежі захисту на підприємстві

На підприємствах з метою зменшення ймовірності несанкціонованого доступу до різних частин підприємства, реалізований метод створення рубежів захисту. Територія компанії ділиться на кілька зон, які ранжовані за рівнем секретності та рівня доступу. У результаті має можливість для розмежування доступу до важливих інформаційних ресурсів.

1.3. Джерела внутрішніх загроз і канали витоку інформації.

Загрози самі по собі не з'являються. Усі загрози можуть бути реалізовані лише за наявності якихось слабких місць – уразливостей, властивих об'єкту інформатизації. Вразливість – деяка слабкість, яку можна використовувати для порушення інформаційної автоматизованої системи чи інформації що міститься у ній.

Джерелами внутрішніх загроз є:

1. Співробітники організації;

2. Програмне забезпечення;

3. Апаратні засоби.

Внутрішні загрози можуть виявлятися в таких формах:

- помилки користувачів та системних адміністраторів;
- порушення співробітниками фірми встановлених регламентів збору, обробки, передачі та знищення інформації;
- помилки у роботі програмного забезпечення;
- відмови та збої у роботі комп'ютерного устаткування.

Джерела загроз можуть бути як всередині об'єкта інформатизації – внутрішні, так і поза ним – зовнішні.

Джерелами внутрішніх загроз виступають:

- порушення персоналом режимів безпеки;
- відмови та збої апаратних засобів і носіїв інформації;
- помилки програмного забезпечення;
- діяльність спільних злочинних угруповань та осіб і ін.

Для реалізації загроз можуть бути застосовані фізичні, радіотехнічні, формаційні і програмні засоби.

До фізичних засобів відносять:

- знищення та руйнування засобів обробки інформації;
- розкрадання апаратних і програмних ключів, добування зразків;
- вплив на персонал.

До радіотехнічних засобів відносять:

- перехоплення інформації в каналах зв'язку;
- радіоелектронне придушення й ін.

До інформаційних засобів відносять:

- несанкціоноване проникнення;
- порушення регламенту інформаційного обміну;
- розкрадання з баз даних і ін.

До програмних засобів відносять:

- впровадження комп'ютерних вірусів;

- впровадження програмних закладок;
- використання операційних і функціональних дефектів;
- дешифрування й ін.

З точки зору етапу життєвого циклу АС, на якому відбувається реалізація загрози, розрізняють загрози:

- впроваджуються на етапі проєктування АС;
- впроваджуються на етапі створення АС (реалізації проєкту);
- впроваджуються на етапі експлуатації АС.

По виду завдання шкоди розрізняють:

- загрози, що завдають явну шкоду, - тобто що полягає в безпосередній втрати цінності оброблюваної інформації;
- загрози, що завдають непрямий збиток, - в цьому випадку, як правило, виводяться з ладу апаратура і програмне забезпечення, тобто матеріальні ресурси, пов'язані з обробкою інформації, а цінність самої інформації не втрачається;
- загрози, що завдають непрямий збиток, - промислове шпигунство, розкрадання програмно-апаратного забезпечення і документації, моральний збиток.

Однак основною ознакою класифікації загроз є їх спрямованість, тобто шлях, яким здійснюється зменшення цінності оброблюваної інформації. **Тут виділяють:**

1. загрози порушення конфіденційності;
2. загрози порушення цілісності;
3. загрози порушення доступності.

Виділяють два напрямки реалізації загроз порушення конфіденційності:

- втрата контролю над системою захисту;
- існування каналів витоку інформації.

Втрата контролю над системою захисту може відбуватися в випадках апаратно-програмного збою в системі, злому системи захисту, оперативних

заходів, штучного або стихійного виникнення критичних або позаштатних ситуацій.

Популярні канали витоку інформації

Канали витоку інформації можуть виникати внаслідок дефектів у активній системі захисту, допущених при її проєктуванні або реалізації.

До найпоширеніших канали витоку відносяться:

- канал витоку по пам'яті - в цьому випадку зловмисник може мати доступ до об'єкта, в який санкціонований користувач записує секретну інформацію;
- канал витоку за часом - в цьому випадку зловмисник може мати доступ до суб'єкта, який представляє інтерес для зловмисника.

Відповідно, можливі витоки також розбиваються на аналогічні три групи.

Серед найпоширеніших каналів витоків даних слід зазначити наступні:

- Електронна корпоративна пошта;
- Інтернет: web-пошта, соціальні мережі, форуми, хмарні сховища;
- Голосові повідомлення: Skype;
- Системи миттєвих повідомлень: WhatsApp, Skype, Microsoft Lync, Jabber, Mail.ru agent, ICQ;
- Файлові сховища: протокол FTP;
- Периферійні та зовнішні пристрої, що підключаються: мобільні пристрої, знімні носії flash, hdd і інші;
- Завдання на друк: локальні й мережеві.

З контролем і захистом усіх зазначених каналів відмінно впорається грамотно налаштований інструмент - DLP (скорочення від «Data Leak Prevention»), який являє собою систему, яка здійснює в режимі реального часу виявлення і запобігання небажаної передачі конфіденційної інформації по різних каналам (як всередині компанії, так і за її межі), а також контроль таких дій на кінцевих пристроях користувачів.

Специфічні канали витоку інформації

Крім зазначених вище каналів є ще кілька і, не зважаючи на те, що їх набагато менше, - контролювати їх набагато складніше:

- Фотографування екрану з конфіденційною документацією;
- Фотографування або крадіжка надрукованих документів.

Перший спосіб контролю - це заборонити на робочому місці використання будь-яких мобільних пристроїв, оснащених камерою, а також встановлення відеоспостереження на всій території компанії (в т.ч. на робочих місцях, що тягне за собою певні труднощі) - такий метод підійде хіба що державному підприємству із суворим режимом обробки інформації, а не комерційній структурі.

Більш ефективним може стати використання платформи маркування документів, наприклад, такий як Docs Security Suite (DSS).

DSS примусово проставляє візуальні та / або приховані мітки конфіденційності на документи (як електронні, так і надруковані), реєструє всі дії користувача з документом, простежує взаємозв'язок документів, розмежовує і контролює права доступу користувачів на основі матриці доступу міток конфіденційності.

Таким чином, навіть якщо відбудеться витік фотографій, то на підставі міток і історії роботи з документом, яка зберігається в базі даних DSS для подальшого аналізу і розслідування інцидентів, можна буде з високою часткою ймовірності дізнатися джерело витоку. Так же даний продукт відмінно інтегрується з DLP, що дозволить відстежувати потоки документів з мітками конфіденційності за всіма зазначеними раніше каналами. [6]

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

У цій частині розділу автор дав визначення такому терміну як «внутрішні загрози», ознайомив з основними принципами й технологіями їх появи.

Внутрішні загрози - це загрози, які пов'язані зі співробітниками організації, тобто людським фактором.

Було визначено, що під внутрішніми загрозами інформаційної безпеки розуміються загрози з боку співробітників компанії як навмисні (шахрайство, крадіжка, спотворення чи знищення конфіденційної інформації, промислове шпигунство тощо), так і ненавмисні (зміна або знищення інформації через низьку кваліфікацію співробітників або неуважність), а також збої програмних чи апаратних засобів обробки та зберігання інформації.

Дослідив джерела та канали витоку інформації, розглянув типову модель порушника інформаційної безпеки підприємства.

Модель порушника - абстрактний (формалізований або неформалізований) опис порушника правил розмежування доступу.

Також автор провів класифікацію внутрішнього порушника ІБ це:

- Ті, хто вважає, що їм не доплачують.
- Ті, хто вважає, що має обіймати вищу посаду.
- Ті, хто вважає, що його не поважають особисто або не зважають на його думку.
- Ті, хто заздрить добробуту роботодавця.
- Ті, хто просто звикли за властивостями свого характеру шкодити, де це можливо.
- Ті, хто незадоволений роботою в компанії з якоїсь іншої причини.
- Ті, хто зібрався звільнитися.

Було розглянуто можливості використання популярних та специфічних каналів витоку інформації, досліджено принцип появи каналів витоку у активній системі захисту.

РОЗДІЛ 2

МЕТОДИ ТА ІНСТРУМЕНТИ ДЛЯ ОРГАНІЗАЦІЇ ЗАХИСТУ ВІД ВНУТРІШНІХ ЗАГРОЗ НА ПІДПРИЄМСТВІ

2.1. Вектор розвитку внутрішніх атак й тенденції із використання методів та інструментів захисту на вітчизняному та зарубіжному ринку

Кількість атак на облікові дані, а також за їх допомогою продовжить зростати у 2022 році. Головна проблема персоналу, що працює віддалено, пов'язана з безліччю залучених у процесі додатків і сервісів у публічних, приватних та гібридних хмарах, які доступні за межами корпоративного брандмауера. Хакери намагатимуться використовувати права доступу співробітників та підрядників організації, щоб закріпитися у її додатках та даних.

Протидія цим атакам ускладнюється тим, що більшість організацій не мають персоналу, інструментів або пропускної спроможності для виявлення незвичайної поведінки користувачів.

Exabeam вважає, що в поточному році аналітики усунуть основні прогалини у своїх інструментах та методах, і перейдуть до превентивної безпеки. Вони будуть відстежувати не конкретні ризики, а зміни в шаблонах поведінки, що допоможе запобігти втомі від занадто великої кількості помилкових спрацьовувань. Єдиний спосіб перейти до підходу, що ґрунтується на моніторингу тактики, методів або процедур (TTP) зловмисників, це використовувати просунуті можливості поведінкової аналітики.

За оцінками аналітиків DX Agent, у 2020 році обсяг українського ринку рішень інформаційної безпеки зменшився на 22% і склав орієнтовно $ 68 млн в цінах замовників (для порівняння: у 2019 році він зріс на 52% і досяг $ 86 млн).

Як наголошується, в структурі продажів як і раніше переважає ПО з часткою 57% ($ 38,8 млн), чверть припадає на апаратно-програмні рішення ($ 16,8 млн), причому, саме їх продажі впали на 49%, а ось частка послуг виросла на два пункти - до 18% ($ 12 млн).

Рис 2.1. Показники українського ІБ-ринку, дані DX Agent

Що стосується вендорів, то склад п'ятірки лідерів не змінився: як і рік тому, це Cisco, Check Point Software Technologies, Fortinet, Symantec і Eset. Однак їх сумарна частка впала з 56% у 2019 році до 50% у 2020-м Серед великих замовників, як і роком раніше, лідирує «Ощадбанк» з часткою 17-18%.[7]

Тенденції у сфері кібербезпеки

1. Віддалена робота, кіберграмотність. Більшість компаній поступово звикають до віддаленого чи гібридного формату роботи. Деякі з них кажуть, що готові перевести частину відділів на постійну віддалену роботу. Насамперед це свідчить про поступове розв'язання проблеми низької кіберграмотності працівників. Безперечно, це тренд 2021 року.

2. Витрати на кібербезпеку зростуть. Висока ймовірність того, що ринок буде змінюватися так швидко, як припускали багато російських та іноземних дослідників наприкінці минулого року: витрати, пов'язані з кіберзлочинністю, можуть досягти 6 трлн дол. у світі і близько 7 трлн руб. в Росії. Понад 50% вітчизняних компаній вже повідомили, що збільшать бюджет на інформаційну безпеку, 42% мають намір розширити відділи кібербезпеки.

3. Ризик-орієнтованість. Компанії почали вибудовувати політику щодо кібербезпеки, ґрунтуючись не на загальновідомих положеннях, а на власних

бізнес-ризиках і кіберризиках. Це пов'язано, по-перше, зі стрибком кіберкомпетентності багатьох представників бізнесу (компетентні в цьому питанні компанії у 2020 році були змушені «навчитися»), а по-друге — з витратами на інформаційну безпеку, які незмінно зростають, які можна оптимізувати, тільки знаючи напевно, які рішення потрібні у конкретних випадках. Ризикоорієнтований підхід дозволить компанії правильно розпорядитися бюджетом та оцінити ефективність інвестицій у кібербезпеку.

4. Криза кадрів у кібербезпеці. Дані досліджень ринку кібербезпеки США на кінець 2020 року підтвердили, що кадрів катастрофічно не вистачає: вакансій у середньому на 50% більше, ніж претендентів. Російський сектор також незабаром відчує цей брак, хоча у 2020 р. у Росії на одну вакансію претендували два кандидати. Але не всі російські компанії вийшли на ту стадію цифрової трансформації, коли розширення відділу інформаційної безпеки стає гострою потребою. Велика ймовірність того, що актуальним тренд стане у найближчі рік-два.

5. Новий виток кібертрансформації. У 2021 р. лідери індустрії розпочали рух у бік власних програмних рішень. Не секрет, що лідери ретейлу та банківського сектора ведуть власні розробки програмного забезпечення, передбачаючи майбутні регуляторні ризики. Важливість подібних рішень насамперед полягає у їхній точній орієнтації на бізнес-завдання та ризики конкретної компанії, всередині якої й розробляється рішення. Зокрема, це допоможе нівелювати частину кіберризиків на рівні програмного коду, забезпечивши значно більший контроль над інфо телекомунікаційною системою та кібербезпекою. Але такий шлях, на жаль, доступний не всім, і у багатьох компаній безпечна архітектура складатиметься із рішень зовнішніх постачальників.

6. Безпека як послуга. Організацію та підтримку роботи системи інформаційної безпеки можна покласти на зовнішню команду фахівців із кібербезпеки (Security as a Service). Сьогодні це не найпоширеніша послуга, але

необхідно враховувати майбутню кадрову недостатність, і тоді ця послуга стане оптимальним рішенням.

7. Кіберзагрози 2021 року. У російському секторі кібербезпеки переважають фішингові атаки, атаки на особисті пристрої віддалених співробітників, а також виявляються програми-вимагачі, шкідливе ПЗ для мобільних пристроїв та інсайдерські витоки. Іншими словами, тенденції кіберзагроз зберігаються. [8]

«Хайпові» тренди в галузі кібербезпеки, які швидко пройдуть та забудуться

Наприкінці травня Gartner назвав 10 головних трендів у сфері кібербезпеки у 2021 році, серед яких було виділено кіберстрахування. На думку фахівців компанії «Лента», цей тренд не буде популярним. Внески у сфері кіберстрахування мають стійку тенденцію до збільшення. Компанії, які не мають більш менш стійкої системи управління ІБ (СУІБ), змушені будуть сплачувати значні внески, які найчастіше значною мірою перевищують бюджети служб інформаційної безпеки. Крім того, «внески» виглядають дуже «лячним» у проєкції на те, що збитки за результатами розбору страхового випадку будуть відшкодовані лише частково, а відновлення процесів та інфраструктури потребує додаткових ресурсів. Що ж до тих компаній, у яких приділяється належна увага кібербезпеці, то, на погляд автора, їм вигідніше вкладати у розвиток СУІБ, ніж щороку сплачувати страхові внески.

Подія в Західній Україні дуже яскраво показало, що рівень кібербезпеки в нашій країні знаходиться в незадовільному стані, і це відноситься як до державних підприємств, так і приватним, причому, не дивлячись на деколи дуже серйозні інвестиції. Очевидно, що це не єдиний випадок масштабних порушень інформаційної безпеки в Україні - просто, що отримав найбільший розголос.

Наприкінці грудня минулого року в Україні сталася безпрецедентна подія: потужна атака хакерів на інфраструктурні енергорозподільні підприємства призвела до масштабного відключення електроенергії. Blackout тривав від 1 до 3 годин у трьох областях і торкнувся понад 220 000 споживачів. Але, як показало

дослідження антивірусних експертів, ця атака не була спонтанною, і підготовка до неї розпочалася ще у травні 2014 року. Саме тоді кіберзлочинці встановили в системі троян і тривалий час збирали інформацію про систему та мережу, відправляючи її у віддалений командний центр.[9]

Найефективніші гравці у сфері кібербезпеки

Ринок кібербезпеки наповнений різноманітними постачальниками, починаючи від великих постачальників платформ, які пропонують цілісну безпеку, до менших постачальників, які пропонують вузькоспеціалізовані рішення в певних областях кібербезпеки.

Наступні компанії виділяються як одні з найефективніших гравців у сфері кібербезпеки:[10]

- *Palo Alto Networks*
- *Fortinet*
- *Cisco*
- *Crowdstrike*
- *IBM*
- *Okta*
- *Dynatrace*
- *Trend Micro*
- *Broadcom Symantec*
- *McAfee*
- *RSA*
- *Cybereason*
- *VMware*
- *Intel*

9 важливих тенденцій кібербезпеки на 2022 рік

1. Підвищення обізнаності користувачів

Зі збільшенням тяжкості кіберзлочинності декілька фірм розробили стратегії для підвищення безпеки своєї організації, збереження досвіду своїх клієнтів і досягнення балансу між безпекою та зручністю. Важливо навчати

споживачів виявляти та уникати мережевих атак, щоб зберегти імідж компанії. Багато людей не знайомі зі стратегіями, які використовуються в кібератаках.

Як наслідок, освіта громадськості має вирішальне значення для запобігання подібним нападам. Численні фірми продають і навчають своїх співробітників за допомогою Інтернету, наочних посібників і традиційних методів у класі. Крім того, співробітники проходять навчання щодо того, як обробляти та передавати конфіденційну корпоративну інформацію.

2. Безпека на базі штучного інтелекту

Машинне навчання перетворилося на більш активну структуру і зробило створення надійних протоколів кібербезпеки простішим, менш дорогим і ефективнішим, ніж будь-коли раніше. Штучний інтелект може передбачати й реагувати на атаки, оскільки він може використовувати велику базу даних для створення шаблонів і використання алгоритмів для їх регулювання.

Машинне навчання дає змогу кібербезпеці виявляти ризики та вивчати поведінку кіберзлочинців, щоб запобігти майбутнім атакам. Це також скорочує час, необхідний фахівцям з кібербезпеки для виконання своїх щоденних завдань.

3. Цілеспрямовані фішингові атаки

Фішингові атаки наразі є найбільш поширеною проблемою безпеки в індустрії інформаційних технологій, і велика кількість людей відповідає на фішингові електронні листи. Хоча фішингові електронні листи та шкідливі URL-адреси залишаються поширеними в Інтернеті, останніми роками вони стали більш конкретними, персоналізованими та географічними. Вони вимагають розгортання шахраями все більш складної тактики для створення добре виконаних кампаній компромісу корпоративної електронної пошти.

Згідно зі звітом Verizon про розслідування порушень даних за 2019 рік, минулого року 32% порушень даних сталися через спроби фішингу (NIST 2019). Як наслідок, експерти з безпеки очікують, що цілеспрямований фішинг стане популярним у наступні роки. Крім того, варто зазначити, що у 2020 році було понад 60 000 фішингових вебсайтів, і кожен восьмий співробітник ділився інформацією про фішинговий сайт

В результаті організації впроваджують і інвестують у комплексні програми підвищення обізнаності щодо безпеки. Крім того, компанії встановлюють симулятори, які можуть пояснити та передбачити розвиток тенденцій фішингу та методів кіберзлочинця.

4. Використання мобільних пристроїв як вектор атаки

Мобільні платформи використовуються для доступу до більшості програмного забезпечення електронної комерції та інших платформ. Кіберзлочинці націлені на мобільних користувачів, експлуатуючи мобільні пристрої як вектори атаки. Оскільки мобільні користувачі використовують свої пристрої для ділового та особистого спілкування, покупок, бронювання готелів та банківської діяльності, кіберзлочинці вважають їх легкою мішенню. Мобільні пристрої зазвичай використовуються як вектор атаки кіберзлочинцями. Понад 70% всіх транзакцій є шахрайськими на мобільних пристроях.

5. Загрози вищій освіті

Кібербезпека стала критичним елементом для студентів, які здобувають вищу освіту в ці неспокійні часи, особливо у зв’язку зі зростанням онлайн-навчання та віддаленої роботи. Компроміс студентських даних є найбільш поширеними тенденціями кібербезпеки у вищій школі. Цього року три приватні заклади піддалися атаці хакера, який викрав дані про вступ студентів (Inside Higher Ed, 2019). Особи, що працюють у сфері вищої освіти, усвідомлювали важливість енергійної кампанії за підвищення інституційної безпеки для захисту даних студентів, викладачів та наукових досліджень.

6. Уразливість Інтернет речей (IoT)

Більшість пристроїв Інтернету (IoT) на ринку сьогодні мають проблеми з безпекою. Через комп’ютерні блоки, інтегровані в елементи IoT, дані можуть передаватися та отримуватися через Інтернет. Як наслідок, користувачі вразливі до DoS-атак і викрадення пристроїв. Вторгнення в будинок є однією з найбільш тривожних небезпек, пов'язаних з Інтернетом речей. У результаті пристрої IoT пропонують нові можливості як бізнесу, так і кіберзлочинцям.

7. Кібератаки на фінансові послуги

Конкретні фінансові організації продовжують докладати зусиль для дотримання правил і переходу на хмару. Спроби фішингу також впливають на фінансових гравців у соціальних мережах та інших каналах зв’язку. На додаток до фішингових атак, фінансові організації вразливі до злому даних і вірусних атак. Фінансові системи більш вразливі до кібератак, ніж інші підприємства, що коштує кожній корпорації в середньому 18,3 мільйона доларів.

8. Уряди пообіцяв будувати екологічні мережі 5G

Сьогоднішня цифрова революція дуже залежить від підключення пристрою для обміну даними та самоконтролю (зазвичай званий IoT). Для ефективного виконання цього потрібна високопродуктивна мережа, а технологія 5G (або, можливо, 6G) добре підходить для цієї роботи.

Справді, враховуючи залежність розумного міста від телекомунікацій, де все пов’язано, кілька урядів проголосили мережі 5G національною інфраструктурою. Їхня безпека стала питанням національної оборони. Коротко кажучи, «безпека за проєктом» має вирішальне значення для захищеної мережі 5G, що розв'язує проблеми безпеки на ранньому етапі.

Після спалаху COVID-19 схоже, що все більше країн слідкують за урядом США, визнаючи китайські компанії, такі як Huawei, ненадійними постачальниками. Хоча такі випадки можуть випливати з політичних міркувань, одне можна сказати точно: вони не зникнуть найближчим часом.

9. Порушення ланцюга постачання

Ніхто не знає, яким буде майбутнє тенденцій кібербезпеки, і багато галузей все ще борються із захистом своїх мереж на тлі хаосу та невизначеності пандемії. Однак чині тенденції дають змогу зрозуміти, чого очікувати в найближчі роки. Розробники та адміністратори продуктів безпеки інформаційних технологій залишаться популярними протягом багатьох років.

Хоча компанії повинні створювати свої групи безпеки, також важливо пам'ятати, що кібербезпека – це справа кожного! Розгляньте можливість фішингових атак. Згідно з опитуванням, навчені співробітники вп'ятеро рідше натискають на фішингові листи. Щоб захистити ваші найбільш цінні активи,

необхідно з'ясувати, чи ваші співробітники, працівники та клієнти поінформовані про кібербезпеку. І для цього необхідно використати такі стратегії.

Відстежуйте поточну інформацію про кібератаки та тактику захисту. Замість того, щоб намагатися приховати вразливість та конфіденційні знання, поділіться ними зі своєю командою та встановіть безпечні процедури. У світі, де всюди підстерігають небезпеки, єдиний спосіб забезпечити свою безпеку – це співпраця.[11]

Глобальний прогноз кібербезпеки на 2021 рік

Зростання витрат на інформаційну безпеку на 6,4%, до $133,78 млрд – Gartner.

Глобальні витрати на автоматизовані системи забезпечення інформаційної безпеки та управління ризиками (Integrated risk management, IRM) у 2020 році досягли $133,78 млрд, що на 6,4% більше, ніж роком раніше. Про це свідчать дані аналітиків Gartner.

Згідно з опитуванням Gartner, пріоритет у нових витратах є кібербезпека: 61% більш ніж з 2000 опитаних IT-директорів вирішили збільшити інвестиції в інформаційну безпеку.

Послуги в галузі безпеки, включаючи консалтинг, підтримку обладнання, впровадження та аутсорсинг, є найбільшою категорією витрат у 2020 році, що оцінюється більш ніж у $65 млрд. На другому місці знаходяться витрати на захист інфраструктури, зафіксовані на рівні $20,5 млрд.

Третя за розміром стаття витрат компаній у сфері кіберзахисту — це обладнання мережевої безпеки. На нього у 2020 році було витрачено понад $15,6 млрд. Також у Gartner вказують на $12 млрд витрат на системи ідентифікації та управління доступом.

Продажі програмного забезпечення для захисту споживчих пристроїв у 2020 році оцінені в $6,51 млрд. Реалізація рішень для захисту даних склала $2,98 млрд, а найменшою, але швидко зростаючою категорією названо технології хмарної безпеки, витрати на які у 2020 році дорівнювали $595 млн.

Аналітики Gartner серед найбільш перспективних розробок у галузі хмарного ІБ виділяють три технології: SASE, CSPM та CASB.

Для управління гібридними та мультихмарними середовищами служать рішення класу Cloud Security Posture Management (CSPM), які забезпечують захист та моніторинг спільної роботи рішень від кількох постачальників IaaS або PaaS (у тому числі дозволяє контролювати доступ, оцінювати політики відповідності вимогам, виконувати оперативний моніторинг, реагувати на інциденти, виконувати ідентифікацію та візуалізацію ризиків, а також інвентаризацію та класифікацію активів). [12]

Information Security & Risk Management End User Spending by Segment, 2020-2021 (Millions of U.S. Dollars)

Market Segment	2020	2021	Growth (%)
Application Security	3,333	3,738	12.2
Cloud Security	595	841	41.2
Data Security	2,981	3,505	17.5
Identity Access Management	12,036	13,917	15.6
Infrastructure Protection	20,462	23,903	16.8
Integrated Risk Management	4,859	5,473	12.6
Network Security Equipment	15,626	17,020	8.9
Other Information Security Software	2,306	2,527	9.6
Security Services	65,070	72,497	11.4
Consumer Security Software	6,507	6,990	7.4
Total	**133,776**	**150,409**	**12.4**

Source: Gartner (May 2021)

Рис 2.2. Витрати на інформаційну безпеку

Інвестиції в ІБ-стартапи досягли $7,8 млрд

Інвестиції в стартапи в галузі кібербезпеки досягли рекордного рівня $7,8 млрд у 2020 році. Зростання насамперед було викликане активністю США –

інвестиції в сектор збільшилися на 22% у 2020 році у порівнянні з 2019 роком. Для порівняння, загальний обсяг венчурних інвестицій за той же період становив 15%. На США припало 76% всього глобального фінансування кібербезпеки у 2020 році, що становить $5,9 млрд, свідчать дані Crunchbase.

На відміну від загального ринку венчурного капіталу, 39% фінансування проєктів у галузі кібербезпеки було спрямоване на стартапи на початковій стадії розвитку. У світовому масштабі цей показник збільшився до 45%.

За повідомленням Crunchbase, географічна різноманітність не вражає, оскільки на США та Ізраїль разом узятих у 2020 році припадало майже 90% всього венчурного фінансування компаній, які займаються кібербезпекою.

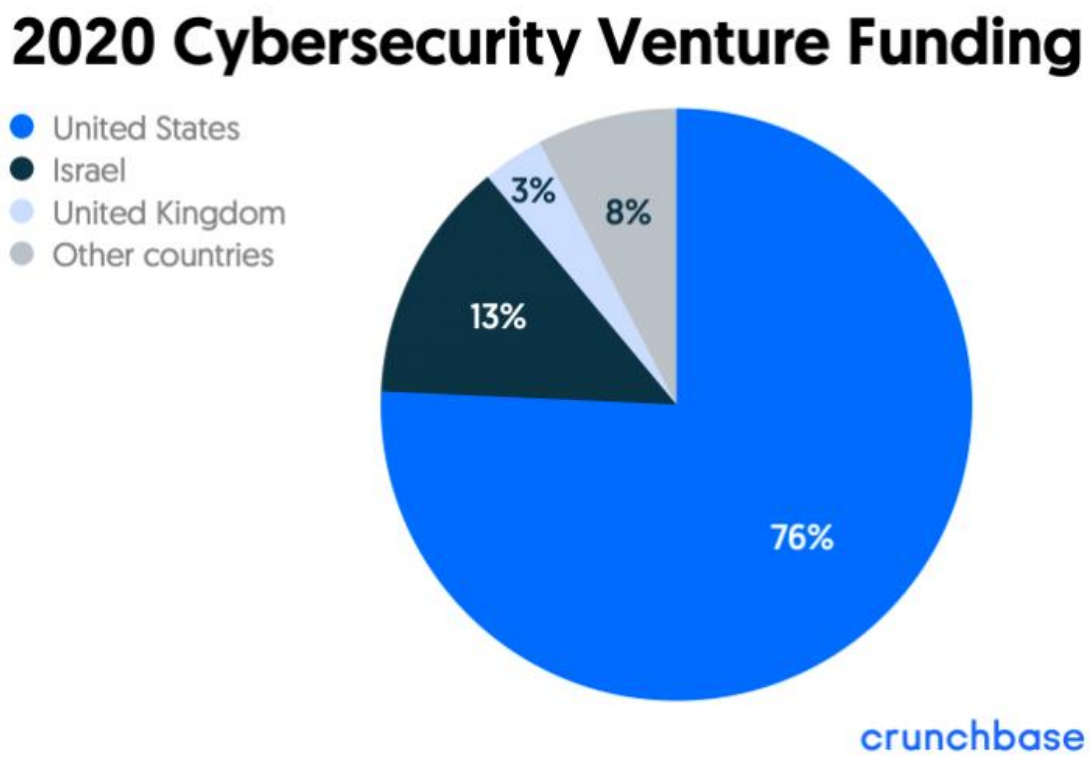

Рис 2.3. Об'ємом венчурного інвестування в стартапи з кібербезпеки (США, Великобританія, Ізраїль та інші.)

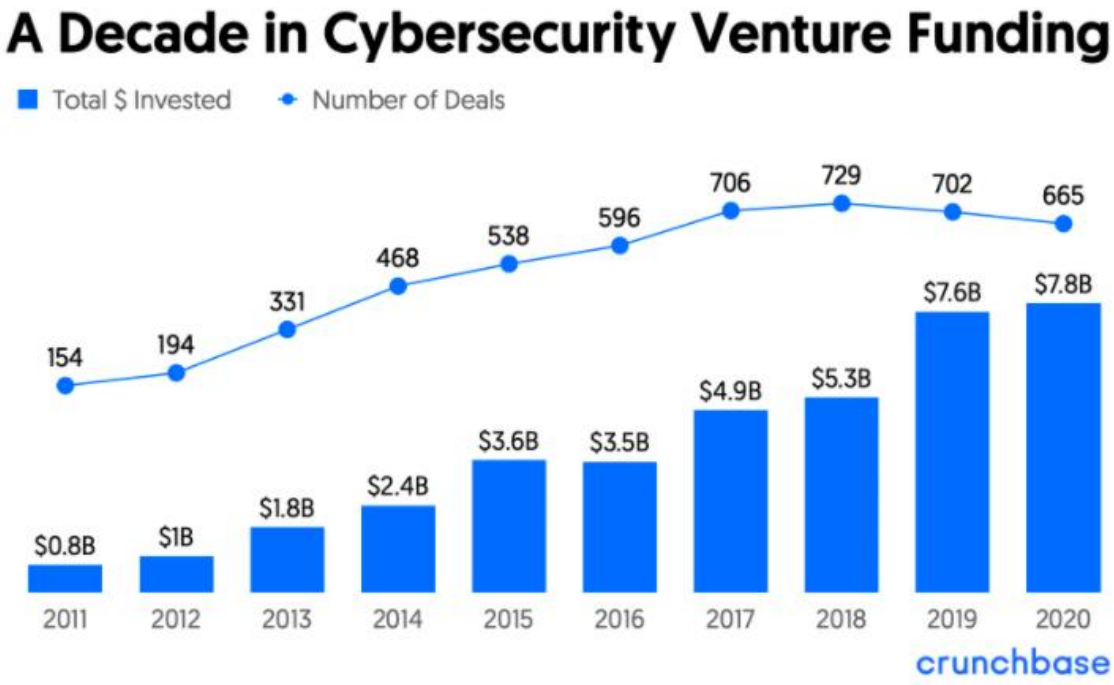

Рис 2.4. Обсяг інвестицій у стартапи з кібербезпеки за 2011-2020 роках.

Витрати компаній на кібербезпеку зросли на 10%, до $53 млрд

У 2020 році компанії у всьому світі інвестували в інформаційну безпеку (ІБ) близько $53 млрд, що на 10% більше, ніж роком раніше. Такі дані навели в дослідній компанії Canalys.

Там зазначили, що за темпами зростання ІБ-рішення випередили багато інших сегментів IT-галузі. Сильніше збільшилися хіба що продажі хмарних продуктів (+20%) та сервісів для побудови хмарної інфраструктури, що пов'язано зі сплеском попиту на такі рішення за умов пандемії коронавірусу COVID-19.

Компанії стали витрачати більше грошей на кібербезпеку в умовах витоків даних, що зростають. У 2020 році, за оцінками Canalys, бізнес втратив понад 30 млрд записів зі своїх баз даних, що вдвічі перевищує обсяг витоків у 2019-му. При цьому середній розмір витоку в глобальному масштабі збільшився з 81 млн до 101 млн записів.

В дослідженні наголошується, що атаки шифрувальників у 2020 році мали трагічні наслідки, оскільки з їх допомогою цілеспрямовано атакувалися медичні установи. Декілька відомих організацій припинили свою діяльність у 2020 році через пандемію COVID-19, а компаніям, що вижили, довелося швидко

адаптуватися до нових умов роботи. Найчастіше це відбувалося на шкоду кібербезпеці та в обхід давніх корпоративних політик, внаслідок чого багато організацій зазнавали атак високоорганізованих та витончених хакерів.

За словами експертів, через неуважність та низьку цифрову грамотність співробітники проходять за фішинговими посиланнями, використовують небезпечні паролі, самостійно намагаються боротися з вірусами-шифрувальниками — наприклад, платять зловмисникам-шантажистам за надання ключів для розшифрування даних, які зазвичай все одно не отримують.

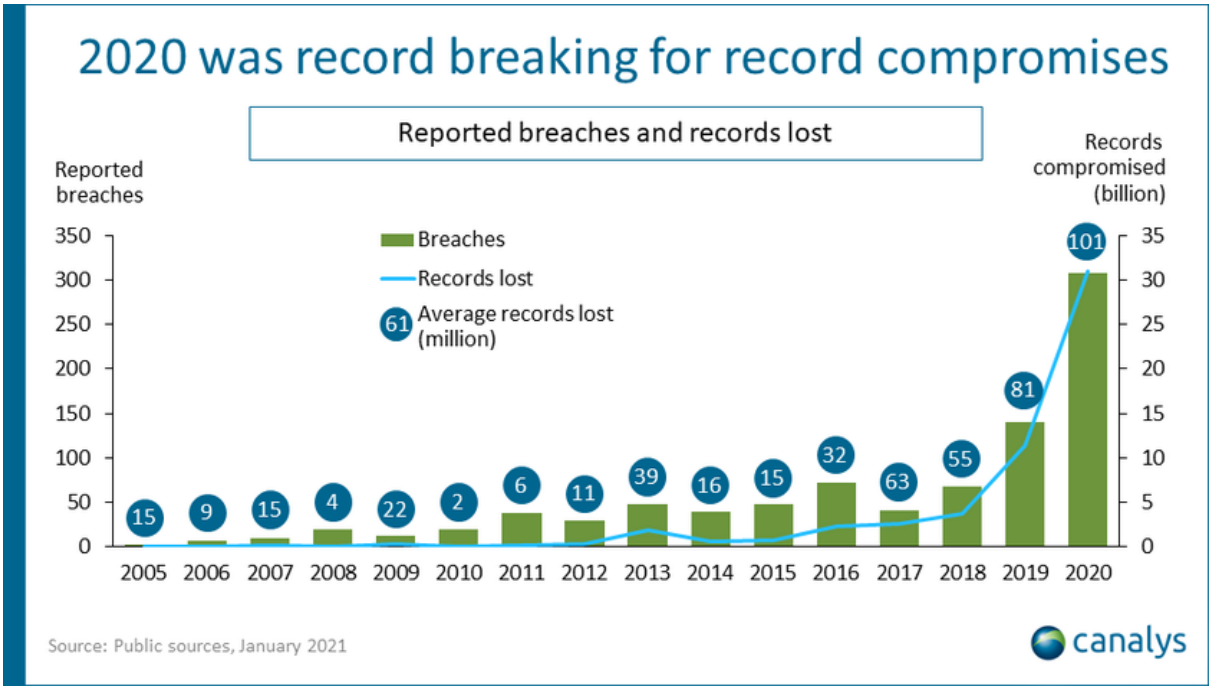

Рис 2.5. Обсяг витоків даних за 2005-2020 роки.

Фахівці кажуть, що з одного боку активізувалися внутрішні порушники, які відчули, що в цифрову епоху дані стали ліквідним товаром на чорному ринку і на них можна заробити. З іншого боку, випадки нелегального використання персональної інформації, у тому числі з шахрайською метою, почали частіше виявлятися завдяки розвитку корпоративних систем безпеки та активній роботі відповідних служб.

Чимала частка крадіжок інформації цього року пов'язана з пандемією коронавірусу — зафіксовано десятки випадків витоку даних хворих COVID-19, контактних осіб, порушників режиму самоізоляції

Пандемія COVID-19 змусила людей залишатися вдома та робити більше покупок через інтернет, а власників бізнесів терміново налагоджувати або розширювати онлайн-продаж. При цьому багато рітейлерів не були готові до такого стрімкого розвитку подій і не мали можливості якісно підготувати інфраструктуру до забезпечення безпеки персональних даних.

Мережева безпека залишилася найбільшим сегментом ІБ-ринку - на її частку припало 36% від усієї суми ІБ-витрат у 2020 році. На цьому напрямі стався спад, що в Canalys пов'язують зі зміною пріоритетів. Закупівлі традиційних апаратних засобів мережевої безпеки підприємств відходять на другий план, оскільки організаціям потрібно збільшувати витрати на кіберзахист від нових вразливостей, що виникають через те, що персонал перейшов на «віддалену роботу».[12]

2.2. Дослідження методів атак на реальних прикладах в контексті внутрішніх порушень

Результати досліджень причин витоку конфіденційної інформації в різних країнах ось уже кілька років є однією і ту ж картину: на першому місці (64% від загального числа розголошення інформації, що захищається) серед джерел витоків завжди стоїть внутрішній порушник - тобто людина, що володіє легітимним правом доступу на територію компанії, яка стає його жертвою.

У 50% випадків - це рядовий співробітник такої компанії, що не володіє набором привілейованих (адміністративних) прав доступу до інформаційних систем.

У 70% випадків відбувається розкриття персональних даних.

В 5 реальних випадках витоків даних для виявлення цих інцидентів за приклад використовується рішення від StaffCop.

Staffcop - програмне рішення, що виконує збір та аналіз інформації з функціональністю DLP та SIEM. Для роботи StaffCop Enterprise потрібен лише один сервер під керуванням ОС сімейства GNU/Linux, призначений для збирання, зберігання, аналізу та перегляду інформації про активність користувачів.

Підключення до сервера здійснюється через захищене з'єднання. Підтримується робота на будь-яких мережних інфраструктурах, які забезпечують підключення від клієнта до сервера: через VPN, NAT та інші канали з'єднання. [13]

Програма агент запускається на робочих станціях або термінальних серверах з операційною системою Windows, відстежує дії користувача та події на його комп'ютері, передає їх на сервер, а також реалізує різні блокування та заборони доступу. Агент StaffCop Enterprise може працювати на віддаленому комп'ютері, що не знаходиться у локальній мережі компанії.

5 реальних випадків витоків даних і їх наслідки

Waymo і їх колишній співробітник

Ентоні Левандовські був провідним інженером у Waymo, автомобільному проєкті Google. У 2016 році він покинув компанію та організував своє підприємство Otto, в рамках якого розроблялися саморушні вантажівки. Через кілька місяців стартап був придбаний фірмою Uber, і Левандовські призначили відповідальним за відділ безпілотних автомобілів. Схоже, це було не раптовим кроком, а ретельно спланованими діями.

Левандовські вкрав у Google і передав в Uber наступні секрети:

- діаграми й малюнки симуляцій, технології радарів і методику LIDAR (виявлення і визначення дальності світла);
- фрагменти вихідного коду;
- конфіденційні PDF-документи;
- відео про тестові поїздки;
- маркетингову інформацію.

Uber вже був готовий закрити операцію з Otto, коли Google нарешті виявила, що Левандовські підключав свій ноутбук до сервера, де зберігалася цінна інформація, завантажив близько 14,000 файлів і скопіював їх на свій диск.

Як такий витік міг відбутися?

Схоже, що служба безпеки не вела моніторинг привілейованих користувачів. Левандовські завантажив файли на свій ноутбук, і ніхто цього не виявив аж до проведення розслідування.

Як цей витік вплинула на компанію?

В рамках проєкту Waymo с 2009 по 2015 роки Google витратила 1,1 млрд доларів США, щоб розробити технологію, яку згодом ледь не втратила. Компанії вдалося довести, що її дані були вкрадені, і отримати компенсацію в розмірі 245 млн доларів від Uber. Також сторони домовилися, що Uber не використовуватиме дані Waymo у своїх розробках.

Як можна було вчасно виявити витік даних?

Особливістю DLP (Data Leak Prevention) є те, що витік даних можна запобігти ще до самої спроби крадіжки.

Розглянемо ситуацію на прикладі StaffCop - системи моніторингу і захисту інформації. В такому випадку користувач був привілейованим і використовував особистий ноутбук. Але що було б, якщо агент DLP працював безпосередньо на сервері з конфіденційною інформацією? Співробітники служби безпеки змогли б отримати повідомлення вже під час копіювання цієї інформації на сторонній носій.

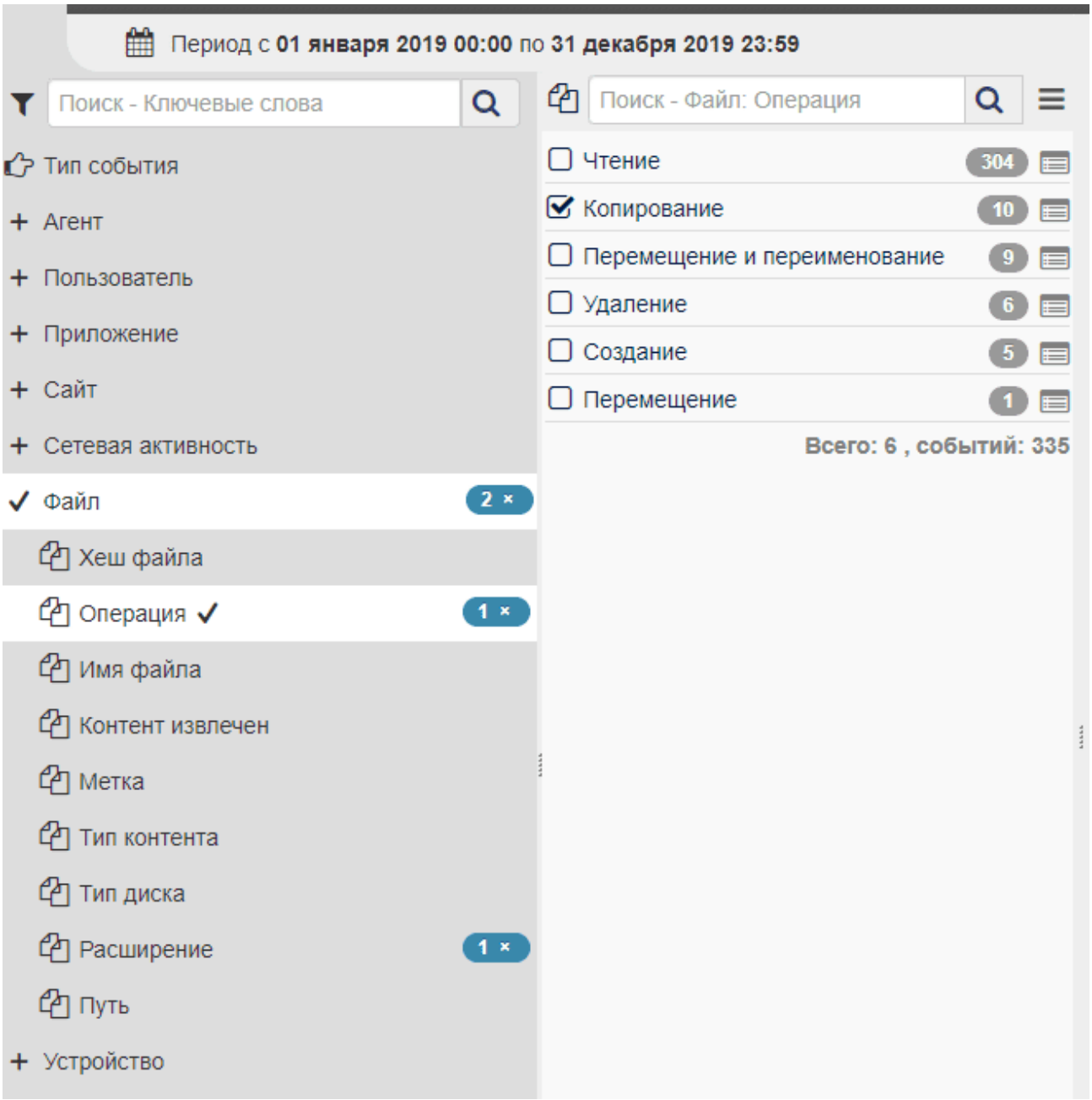

Рис 2.6. Перегляд певних подій за конкретний період

Allen & Hoshall і їх вкрадені секрети

В даному прикладі не буде мільярдних оборотів або інноваційних технологій. Однак він показує характерний варіант розвитку подій в маленьких компаніях.

Джейсон Нідхем, який покинув компанію Allen & Hoshall у 2013 році, організував підприємство HNA Engineering. Разом з тим він продовжив підтримувати відносини з одним з колишніх колег. Це дало Нідхем можливість періодично звертатися до мережевих дисків і користуватися поштою свого

колишнього місця роботи, завантажуючи звідти інформацію про проєкти, фінансові документи й проєкти інженерів (в цілому - 82 документів AutoCAD і близько 100 PDF-документів). A & H не змогла відстежити його дії, і, можливо, вони б тривали досі- але у 2016 році потенційний клієнт отримав від HNA Engineering пропозицію, підозріло схоже з інтелектуальною власністю Allen & Hoshall. Тоді компанія звернулася в ФБР, яке відстежило зловмисника і пред'явило йому обвинувачення у квітні 2017 року.

Як такий витік міг відбутися?

Allen & Hoshall мала непогану систему роздачі прав доступу. Ці права видавалися тільки тим людям, яким дійсно потрібно було працювати з тією чи іншою інформацією. Крім того, облікові дані Нідхема були видалені після його звільнення. Однак Нідхем отримав доступ до пошти колишнього колеги, який все ще працював в компанії.

Як цей витік вплинула на компанію?

Суд порахував, що вартість вкрадених даних варіювалася від $ 250 000 до $ 550 000. Нідхема визнали винним і зобов'язали виплатити компанії Allen & Hoshall 172 тисячі доларів США.

Як можна було запобігти витоку даних?

Компанія не використовувала двофакторную аутентифікацію, що дозволило використовувати обліковий запис співробітника без додаткової авторизації. StaffCop в цьому прикладі теж міг би допомогти виявити витік. Однією з функцій DLP-рішення є контроль файлових операцій на FTP-серверах. Відразу після появи аномальної активності на FTP-ресурсі співробітники служби безпеки змогли б отримати не тільки дані про підключення, але й IP-адреса зловмисника.

2019-09-18 16:20:22	FTP	Win10NOD (1.72)	user	filezilla.exe	Login: anonymous Password: anonymous@example.com Host: 91.122.30.115 Документ.docx Скачать Документ.docx
2019-09-17 11:05:23	FTP	Win10KES (1.24)	user	filezilla.exe	Login: anonymous Password: anonymous@example.com Host: 213.180.204.183 10MB.docx Скачать 10MB.docx

Рис 2.7. Журнали StaffCop, де видно IP-адреса зловмисника

Anthem і постачальники

У 2017 році друга за розміром страхова медична компанія в США постраждала від витоку інформації через стороннього постачальника.

Фірма LaunchPoint, що займається координацією страхових послуг, повідомила про те, що один зі співробітників відправив файл з персональними даними клієнтів на свій особистий ящик. Невідомо, чи були ці дані використані не за призначенням. В цілому постраждало близько 18 580 клієнтів. Були відправлені їх номери договорів, дати народження та інша (медична) інформація.

LaunchPoint надала жертвам два роки безкоштовного моніторингу з витоків особистих даних.

Як такий витік міг відбутися?

LaunchPoint допустила витік даних, бо їх співробітник мав доступ до персональної інформації й міг відправити її на свою особисту пошту. Anthem повинна була вибрати страхового координатора з вищим рівнем безпеки персональних даних.

Як цей витік вплинув на компанію?

Всі фінансові збитки понесла компанія LaunchPoint, але Anthem зіткнулася з репутаційних збитком.

Як можна було запобігти витоку даних?

Засоби моніторингу і DLP забезпечують повний контроль поштових каналів витоку інформації. Наприклад, можна отримувати повідомлення про надсилання листів самому собі або некорпоративних адресатів.

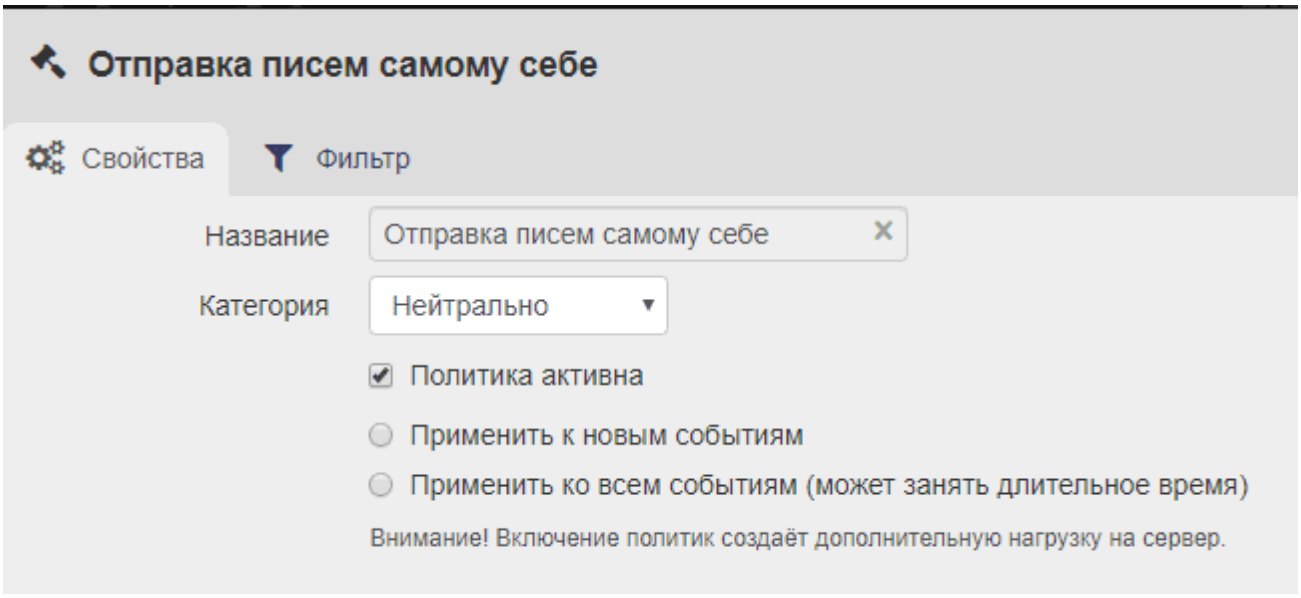

Рис 2.8. Налаштування повідомлень про надсилання листів самому собі

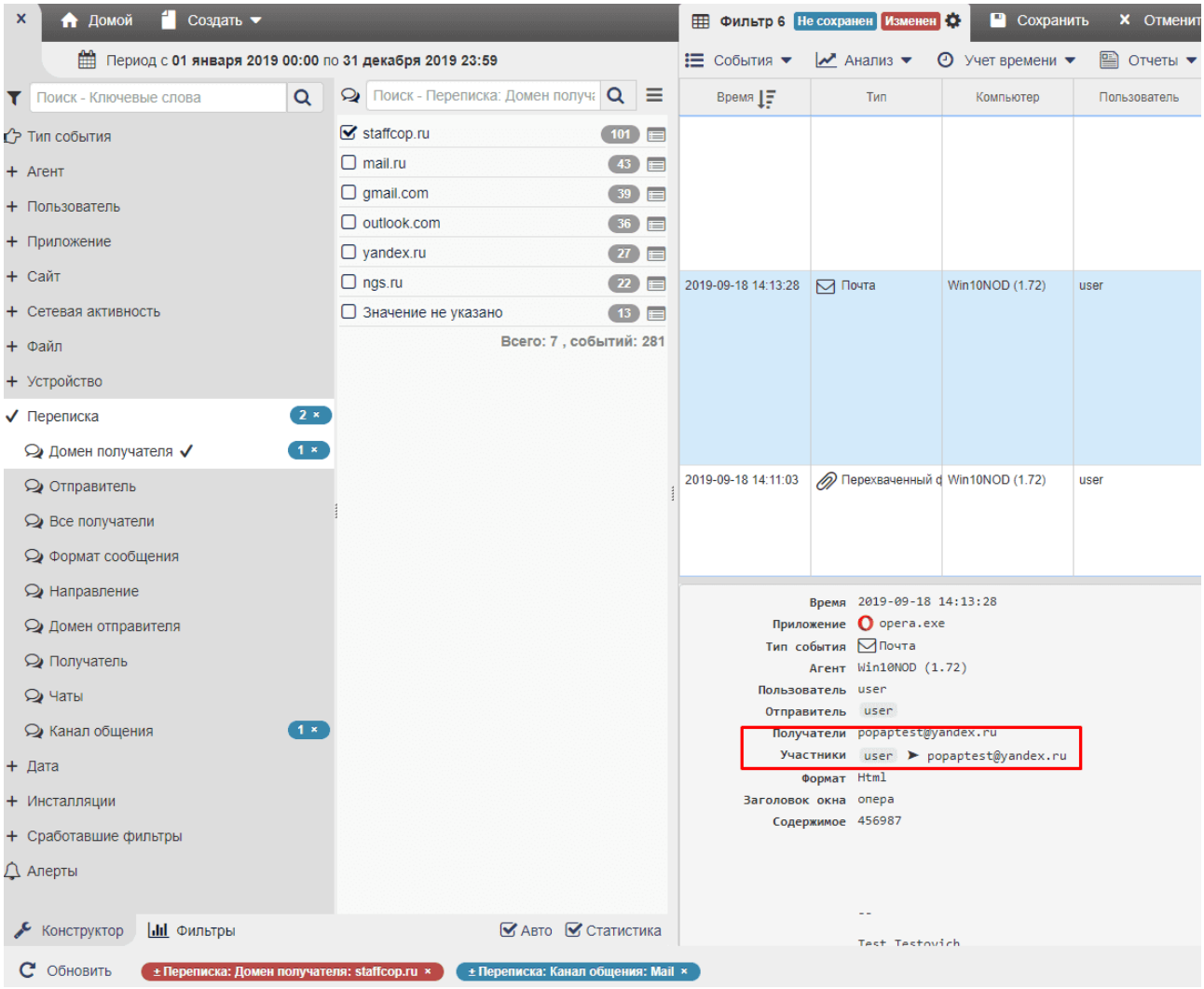

Рис 2.9. Налаштування повідомлень про надсилання листів на некорпоративні адреси

Дані політики дозволяють не тільки оперативно отримувати інформацію про факти надсилання таких повідомлень, а й помічати передачу конкретних персональних даних завдяки пошуку за ключовими словами та регулярними виразами.

Fresenius Medical Care і їх слабка політика безпеки

Компанія Fresenius Medical Care, постачальник продуктів і послуг для людей з хронічною нирковою недостатністю, постраждала від серії невеликих витоків даних через недотримання інструкцій з безпеки. В даному прикладі постраждав 521 людина, і при цьому протягом всього лише одного року було виявлено 5 витоків. Застосування політик інформаційної безпеки щодо захисту персональних даних клієнтів виявилося провальним:

- особисті дані користувачів зберігалися на комп'ютерах в незашифрованому вигляді;
- в одного співробітника вкрали з машини ноутбук з персональними даними;
- в іншого працівника викрали флеш-накопичувач з персональними даними 245 клієнтів;
- жорсткий диск з персональними даними 35 клієнтів був вкрадений під час технічного обслуговування в компанії.

Всі ці крадіжки сталися у 2012 році. Інформація про витік з'явилася тільки у 2018 році.

Як такий витік міг відбутися?

Співробітники могли вільно копіювати персональні дані на особисті ноутбуки та флешки, використовувати їх безконтрольно. Відомості не були зашифровані.

Як цей витік вплинула на компанію?

Fresenius Medical Care заплатила постраждалим три з половиною мільйони доларів США.

Як можна було запобігти витоку даних?

В українському законодавстві немає вимог про обов'язкове шифрування персональних даних користувачів. Однак можна знизити ризики, керуючи правами співробітників і їх поводженням з персональними даними, обмежуючи безконтрольну передачу інформації на знімні носії - наприклад, налаштувати білий список USB-пристроїв, створити окрему категорію документів з обмеженим доступом і видати права лише певної групи відповідальних працівників.

Реалізація таких політик безпеки можлива за допомогою StaffCop.

Конфігурація агентів дозволяє налаштувати білий список USB-пристроїв або ж заблокувати USB-пристрої як клас.

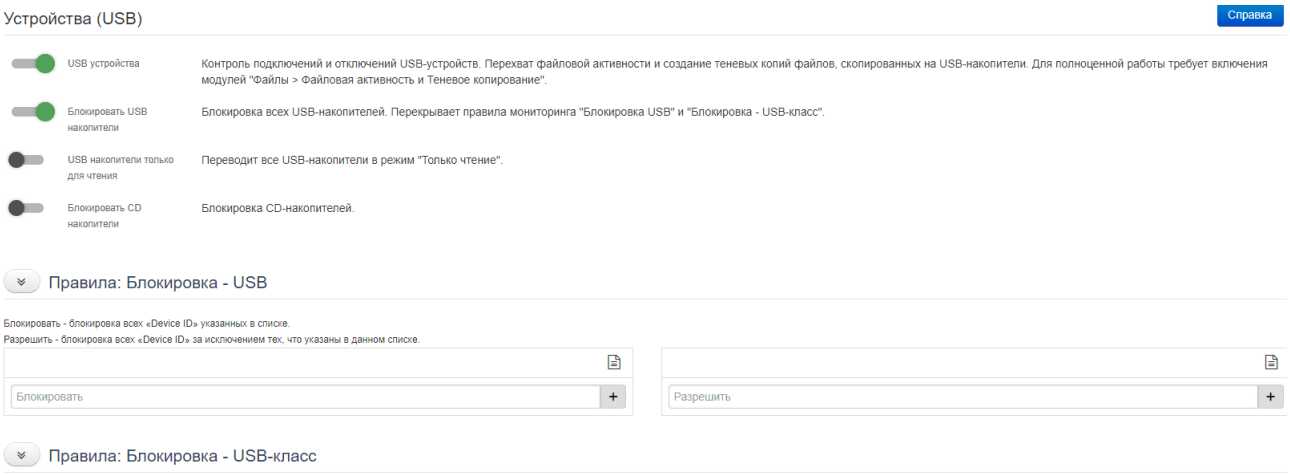

Рис 2.10. Налаштування USB-пристроїв

Виділити документи в окрему категорію, наприклад «Конфіденційно», дозволяє інший модуль - «Мітки й контроль доступу».

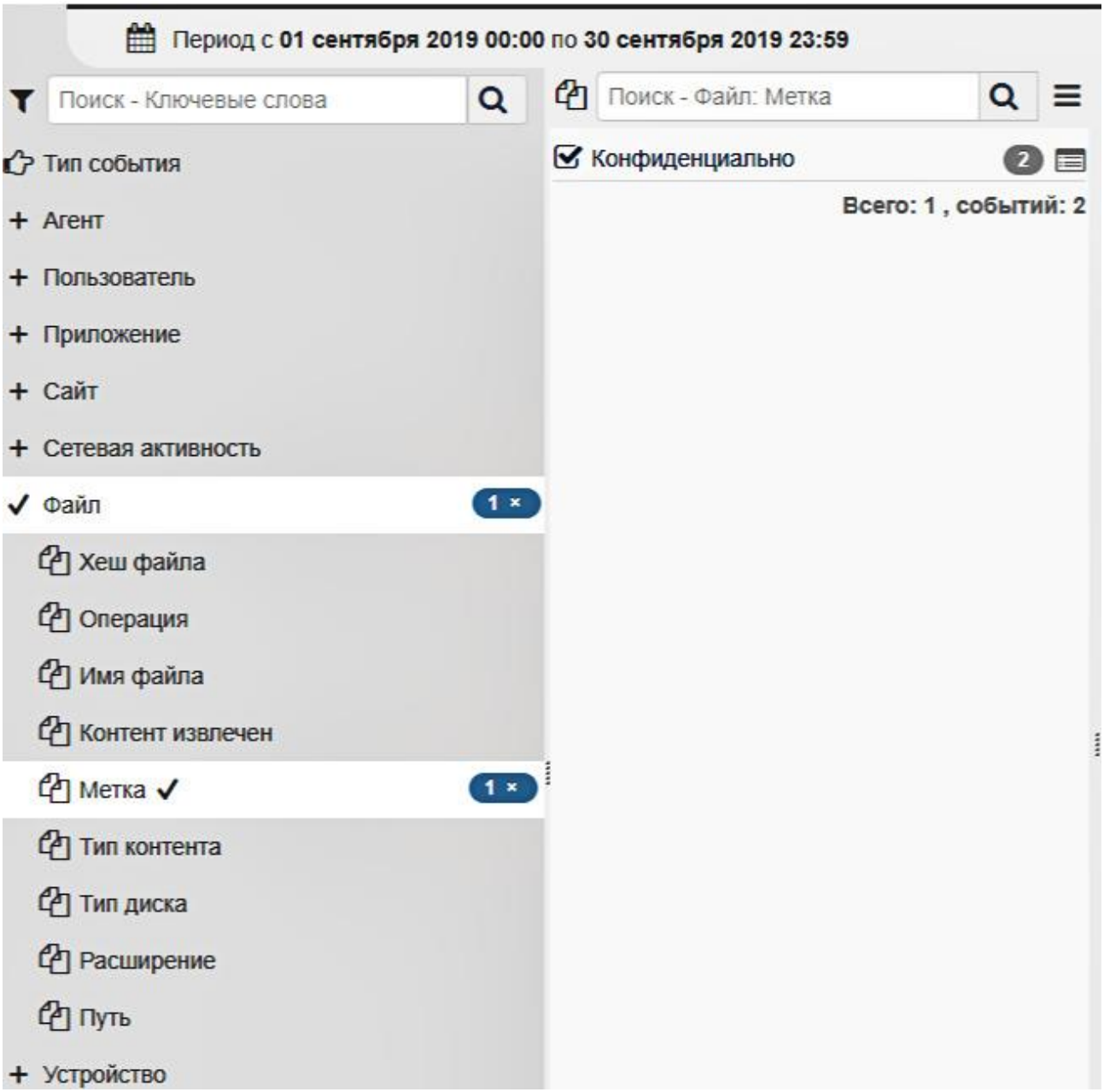

Рис 2.11. Виділення документів в окрему категорію

Згрупувавши захищаєму інформацію і налаштувавши повноцінний нагляд за такими групами документів, можна знизити ризик витоку даних і, що ще більш важливо, вчасно отримати відомості про подібний інцидент.

AMSC і їх китайські конкуренти

Дуже цікавий приклад, який розкриває тенденцію китайських компаній красти комерційні секрети й використовувати їх у своїх розробках і технологіях - іноді за підтримки уряду.

Колишній співробітник AMSC Деян Карабасевіч вкрав відомості, які становлять комерційну таємницю, і продав їх в китайську компанію Sinovel за $ 20 000. Також йому пообіцяли шестирічний контракт на 1,7 мільйона доларів.

Карабасевіч був главою інженерно-технічного відділу компанії й часто їздив у справах до Китаю, де одного разу прийняв пропозицію від конкурентів про передачу їм вихідних кодів програмного забезпечення турбіни AMSC.

У березні 2011 року Карабасевіч подав заяву про звільнення з фірми, але протягом ще декількох місяців у нього залишався доступ до серверів AMSC. Пізніше, під час розслідування, з'ясувалося, що Карабасевіч листувався електронною поштою з китайськими конкурентами, обговорюючи вихідні коди. Sinovel зібрали турбіни з програмним забезпеченням на основі розробок AMSC і продали їх в Массачусетс; на щастя, компанія, яка займалася складанням, помітила збіги в коді й повідомила в AMSC. Це сильно допомогло в розслідуванні.

Як такий витік міг відбутися?

Карабасевіч мав привілейований доступ, міг безконтрольно листуватися з конкурентами й часто подорожував до Китаю.

Як цей витік вплинула на компанію?

Після того як дані були вкрадені, компанія втратила свого найбільшого клієнта - Sinovel Wind Group. Китайське підприємство відмовилося від розробок AMSC, вартість акцій якої впала на 84% за кілька місяців. Фінансові втрати склали понад 1 мільярда доларів США. Тільки через 6 років, в січні 2018 року, суд наклав на Sinovel штраф в розмірі 1,5 мільйонів доларів США, а також наказав їй виплатити 57,5 мільйонів доларів компанії AMSC і 850 тисяч доларів - іншим жертвам.

Як можна було запобігти витоку даних?

Контроль всього листування користувачів, особливо тієї частини, яка ведеться з конкурентами, - одна з ключових складових інформаційної безпеки. Відстеження корпоративних і особистих месенджерів, пошти, пошук ключових

слів, пов'язаних з вашою інтелектуальною власністю, - найкращий спосіб не допустити такий витік інформації.

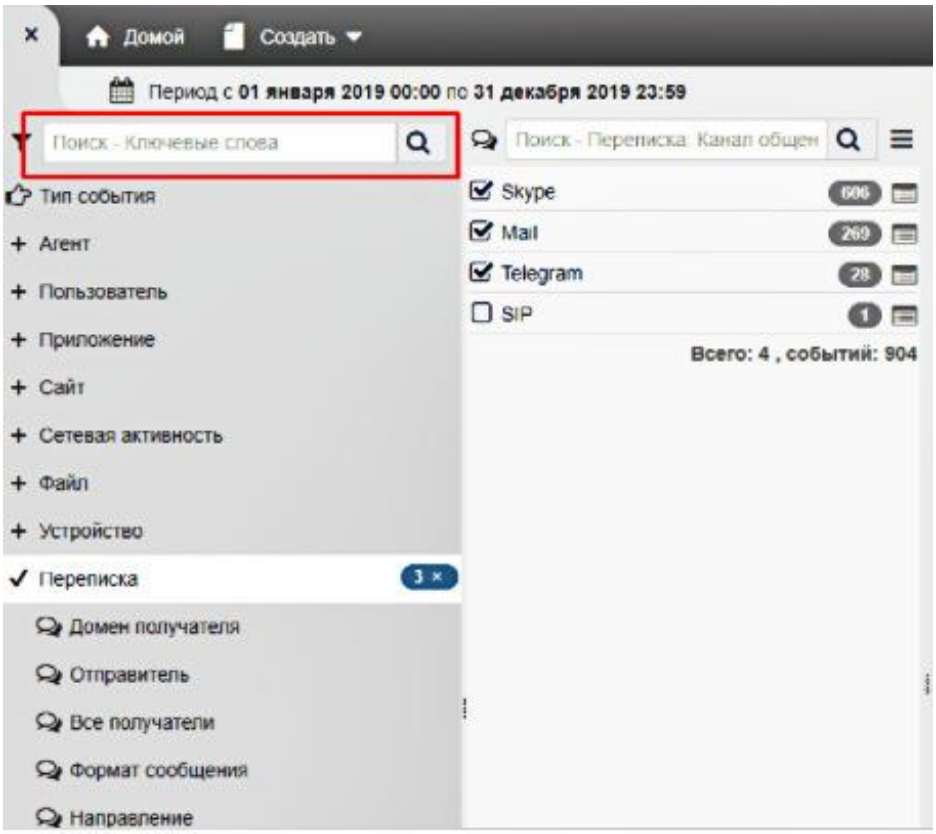

Рис 2.12. Пошук за ключовими словами

Як можна було замітити рішення DLP ефективне якщо розмова іде про контроль дій користувачів, але не дає повної видимості й контролю всіх активів підприємства.[13]

Розглянемо ще декілька випадків витоку персональних даних з різних підприємств та їх сервісів які могли відбутися в контексті внутрішніх порушень. [14]

Випадок №1: витік бази даних Microsoft через недбалість співробітників

Що трапилося?

Наприкінці грудня 2019 року дослідник безпеки виявив загальнодоступну базу даних підтримки клієнтів Microsoft, що містить 250 мільйонів записів, накопичених за 14 років. База даних включала звернення та деталі в службу

підтримки, електронні листи та IP-адреси клієнтів, географічні розташування клієнтів та нотатки, зроблені агентами служби підтримки Microsoft.

База даних була загальнодоступною близько місяця. Microsoft забезпечила безпеку того ж дня, коли було повідомлено про злом.

Які були наслідки?

Оскільки витік даних не містив особистої інформації, а компанія терміново закрила пролом і повідомила порушених користувачів, Microsoft не зазнала жодних штрафів або пені.

Проте Microsoft пощастило, що витік даних з вини інсайдерів було виявлено наприкінці 2019 року. Декілька днів потому, 3 січня 2020 року, набрав чинності Закон Каліфорнії про конфіденційність споживачів. Цей закон накладає штраф у розмірі 750 доларів США на кожну особу, яка постраждала внаслідок порушення. Згідно з новим законодавством, Microsoft могла бути оштрафована на мільйони доларів.

Чому це сталось?

На початку грудня 2019 року Microsoft розгорнула нову версію правил безпеки Azure. Співробітники Microsoft неправильно налаштували ці правила та викликали випадковий витік. Доступ до бази даних не був захищений паролем або двофакторною автентифікацією. Крім того, компанія може значно скоротити час виявлення, відстежуючи записи користувачів і переглядаючи дії з конфіденційними активами.

Випадок № 2: витік даних Marriott через зламаний сторонній додаток

Що трапилося?

У січні 2020 року хакери використовували сторонню програму, яку Marriott використовувала для надання гостьових послуг. Зловмисники отримали доступ до 5,2 мільйона записів гостей Marriott. Ці записи включали контактну інформацію, стать, дні народження, дані облікового запису лояльності та особисті переваги. Наприкінці лютого 2020 року служба безпеки Marriott помітила підозрілу активність та усунула порушення безпеки, спричинене інсайдерами.

Які були наслідки?

На момент написання статті розслідування цього інциденту продовжується. Marriott може мати справу з серйозними штрафами, оскільки вкрадені дані включають особисту інформацію.

Це не перше розслідування витоку даних для компанії: Marriott все ще бореться зі штрафом у розмірі 99 мільйонів фунтів стерлінгів (приблизно 124 мільйони доларів) GDPR за витік даних у 2018 році.

Чому це сталось?

Зловмисники скомпрометували облікові дані двох співробітників Marriott для входу в один зі сторонніх додатків мережі готелів. Системи кібербезпеки Marriott не помічали підозрілі активності профілів цих співробітників протягом двох місяців. Завдяки моніторингу сторонніх постачальників та аналітики поведінки користувачів та організацій, Marriott могла виявити порушення ще до того, як хакери отримали доступ до даних клієнтів.

Кейс № 3: Співробітники General Electric украли комерційну таємницю, щоб отримати комерційну перевагу

Що трапилося?

Два співробітники General Electric (GE) вкрали дані про сучасні комп'ютерні моделі для калібрування турбін, які виробляла компанія. Вони також вкрали маркетингову та цінову інформацію для просування цієї послуги.

З вкраденою інтелектуальною власністю один зі співробітників заснував нову компанію та змагався з GE у тендерах на калібрування турбін.

Які були наслідки?

GE програла новому конкуренту кілька тендерів на калібрування турбін. Коли вони виявили, що цей конкурент був започаткований їхнім співробітником, вони повідомили про інцидент у ФБР. У 2020 році, після кількох років розслідування, інсайдерів було засуджено та засуджено до тюремного ув'язнення та виплати компенсації у розмірі 1,4 мільйона доларів компанії General Electric.

Чому це сталось?

Співробітники GE завантажили тисячі файлів з комерційною таємницею із серверів компанії та відправили їх на приватні адреси електронної пошти або завантажили у хмару. Один співробітник також переконав системного адміністратора надати йому доступ до даних, яких він не повинен мати доступу.

Жодна з цих зловмисних дій не викликала реакції системи кібербезпеки GE. Розгортання рішень для управління доступом та моніторингу активності користувачів могло б допомогти GE вчасно виявити крадіжку інтелектуальної власності та прискорити розслідування шляхом збирання необхідних доказів.

Кейс №4: Колишній співробітник Cisco навмисне пошкодив хмарну інфраструктуру

Що трапилося?

Колишній співробітник Cisco отримав несанкціонований доступ до хмарної інфраструктури компанії та розгорнув шкідливий код, який видалив 456 віртуальних машин, що використовуються для програми Cisco WebEx Teams. В результаті близько 16 000 користувачів WebEx не могли отримати доступ до своїх облікових записів протягом двох тижнів.

Які були наслідки?

Cisco довелося витратити близько 1,4 мільйона доларів робочого часу співробітників на аудит інфраструктури та усунення пошкоджень. Компанії також довелося виплатити потерпілим користувачам компенсацію у розмірі 1 млн доларів.

Інцидент стався у вересні 2018 року, але станом на грудень 2020 року справу досі не вирішено у суді. Зловмиснику може загрожувати до п'яти років в'язниці та штраф у розмірі 250 000 доларів.

Чому це сталось?

Колишній співробітник Cisco використовував свої знання про механізми безпеки Cisco і зловжив їх слабкістю, щоб отримати доступ до хмарної інфраструктури та розгорнути свій код. Зважаючи на все, доступ до конфіденційних ресурсів не був захищений двофакторною автентифікацією або іншими інструментами керування доступом.

Кейс №5: користувачі Twitter займались шахрайством через фішингових співробітників

Що трапилося?

У липні 2020 року хакери отримали доступ до 130 приватних та корпоративних облікових записів Twitter, у кожного з яких не менше мільйона передплатників. Вони використовували 45 з цих облікових записів для просування шахрайства з біткойнами. До списку зламаних облікових записів входять облікові записи Барака Обами, Ілона Маска, Білла Гейтса, Джеффа Безоса, Майкла Блумберга, Apple, Uber та інших відомих осіб та компаній.

Які були наслідки?

Користувачі Twitter перевели на шахрайські рахунки суму, еквівалентну не менше 180000 доларів США в біткойнах. Платформа обміну криптовалюти Coinbase заблокувала перекази ще на 280 000 доларів.

Після інциденту ціна акцій Twitter упала на 4%. Компанія припинила випуск свого нового API для оновлення протоколів безпеки та навчання співробітників атак соціальної інженерії.

Чому це сталось?

Співробітники Twitter стали жертвами цілої мережі фішингових атак. Хакери зібрали інформацію про співробітників компанії, що працюють з дому, зв'язалися з ними, представилися IT-адміністраторами Twitter та запросили облікові дані користувача. Використовуючи ці скомпрометовані облікові записи, зловмисники отримали доступ до інструментів адміністратора. За допомогою цих інструментів вони скидали облікові записи відомих користувачів Twitter, змінювали їх облікові дані та публікували шахрайські повідомлення у Твіттері.

Twitter не помітив підозрілої активності в адмінстративному обліковому записі, поки шахрайські повідомлення не були опубліковані та помічені пресою. Рішення для аналізу поведінки користувачів та об'єктів та управління привілейованим доступом могли б допомогти компанії захистити доступ до інструментів адміністрування та швидко виявити несанкціоновані дії.

Приклади внутрішніх проблем, які ми проаналізували вище, мають одну основну причину: системи кібербезпеки, які не виявляють порушення та не попереджають співробітників служби безпеки до того, як буде завдано реальних збитків.

Загрози безпеки, що походять від інсайдерів, можуть статися з будь-якою компанією. І наслідки порушень, пов'язаних з інсайдерською інформацією, часто бувають руйнівними. Однак у більшості випадків можна виявити та зупинити інсайдерські атаки за допомогою спеціальних інструментів кібербезпеки.[15]

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

Результати досліджень причин витоку конфіденційної інформації в різних країнах ось уже кілька років є однією і ту ж картину: на першому місці серед джерел витоків завжди стоїть внутрішній порушник - тобто людина, що володіє легітимним правом доступу на територію компанії, яка стає його жертвою.

У другому розділі роботи автор розкрив тему витрат та інвестицій в кібербезпеку на вітчизняному та закордонному ринку й проаналізував вектор розвитку внутрішніх атак. Було розглянуто тенденції з захисту інформаційних систем у світі. Дослідив які бувають сценарії витоку даних з внутрішніх систем підприємства, розглянули реальні приклади використання вразливостей та недосконалостей в роботі систем захисту які призвели до витоку конфіденційних та персональних даних.

Було виділено п'ятірку лідерів серед вендорів ІБ продуктів, це Cisco, Check Point Software Technologies, Fortinet, Symantec і Eset.

Також були розглянуті методи, техніки й принципи внутрішніх порушень ІБ. Тепер зрозуміло, як відбуваються витоки даних і як їх можливо було б уникнути.

РОЗДІЛ 3

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЙНИХ АКТИВІВ ВІД ВНУТРІШНІХ ЗАГРОЗ

3.1. Програмно-технічні методи та засоби захисту від витоку інформації

Сьогодні інформаційні технології є важливим складником будь-якої сучасної організації. Говорячи образно, інформаційні технології – це серце підприємства, яке підтримує працездатність бізнесу та підвищує його ефективність та конкурентоспроможність в умовах сучасної, жорсткої конкуренції.

Системи автоматизації бізнес-процесів, такі як документообіг, CRM-системи, ERP-системи, системи багатовимірного аналізу та планування дозволяють оперативно збирати інформацію, систематизувати та групувати її, прискорюючи процеси прийняття управлінських рішень.

Стає очевидним, що велика кількість стратегічних, конфіденційних та персональних даних є важливим інформаційним активом підприємства, і наслідки витоку цієї інформації позначаться на ефективності діяльності організації.

Використання традиційних заходів безпеки, таких як антивіруси й фаєрволи виконують функції захисту інформаційних активів від зовнішніх загроз, але не яким чином не забезпечують захист інформаційних активів від витоку, спотворення або знищення внутрішнім зловмисником.

Внутрішні небезпеки інформаційної безпеки можуть залишатися ігнорованими чи часом непоміченими управлінням через відсутність розуміння критичності цих небезпек для бізнесу. [16]

Саме з цієї причини захист конфіденційних даних такий важливий вже сьогодні.

Програмно-технічні методи захисту виконують такі функції:

- створення перешкод на можливих шляхах проникнення та доступу потенційних порушників до системи та інформації, що захищається;

- ідентифікацію та автентифікацію користувачів;
- розмежування доступу до ресурсів;
- реєстрацію подій;
- криптографічний захист інформації.

Засобами захисту інформації називають пристрої, прилади, пристрої, програмне забезпечення, організаційні заходи, які запобігають витоку інформації та забезпечують її збереження в умовах впливу всього спектра актуальних загроз.

Залежно від використовуваних способів реалізації засоби захисту інформаційної безпеки бувають наступних типів:

Організаційні. Комплекс заходів та засобів організаційно-правового та організаційно-технічного характеру. До перших відносять законодавчі та нормативні акти, локальні нормативні документи організації. Другий тип – це заходи щодо обслуговування інформаційної інфраструктури об'єкта.

Апаратні (технічні). Спеціальне обладнання та пристрій, що запобігає витоку, що захищає від проникнення в IT-інфраструктуру.

Програмні. Спеціальне програмне забезпечення, призначене для захисту, контролю, зберігання інформації.

Програмно-апаратні. Спеціальне обладнання із встановленим програмним забезпеченням для захисту даних.

Найбільшого поширення сьогодні набули програмні засоби захисту інформації. Вони повністю відповідають вимогам ефективності та актуальності, регулярно оновлюються, ефективно реагуючи на актуальні загрози.

Для захисту даних у сучасних мережах використовується широкий спектр спеціалізованого програмного забезпечення. Можна виділити такі типи програмних засобів захисту:

Антивірусне ПЗ. Спеціалізоване ПЗ для виявлення, нейтралізації та видалення комп'ютерних вірусів. Виявлення може виконуватися під час перевірок за розкладом або запущених адміністратором. Програми виявляють та

блокують підозрілу активність програм у «гарячому» режимі. Крім того, сучасні антивіруси можуть відновлювати файли, заражені шкідливими програмами.

Хмарні антивіруси (CloudAV). Поєднання можливостей сучасних антивірусних програм із хмарними технологіями. До таких рішень відносяться сервіси Crowdstrike, Panda Cloud Antivirus, Immunet та багато інших. Весь основний функціонал ПЗ розміщений у хмарі, а на комп'ютері, що захищається, встановлюється клієнт — програма з мінімальними технічними вимогами. Клієнт вивантажує у хмарний сервер основну частину аналізу даних. Завдяки цьому забезпечується ефективний антивірусний захист за мінімальних ресурсних вимог до обладнання. Рішення CloudAV оптимально підходять для захисту ПК, які не мають достатньої вільної обчислювальної потужності для стандартного антивірусу.

Рішення DLP (Data Leak Prevention). Спеціальні програмні рішення, що запобігають витоку даних. Це комплекс технологій, які ефективно захищають підприємства від втрати конфіденційної інформації з різних причин. Впровадження та підтримка DLP – вимагає досить великих вкладень та зусиль з боку підприємства. Однак цей захід здатний значно зменшити рівень інформаційних ризиків для IT-інфраструктури компанії.

Системи криптографії. (DES - Data Encryption Standard, AES - Advanced Encryption Standard). Перетворюють дані, після чого їхнє розшифрування може бути виконане тільки з використанням відповідних шифрів. Крім цього, криптографія може використовувати інші корисні програми для захисту інформації, у тому числі дайджести повідомлень, методи автентифікації, зашифровані мережеві комунікації, цифрові підписи. Сьогодні нові програми, що використовують зашифровані комунікації, наприклад Secure Shell (SSH), поступово витісняють застарілі рішення, що не забезпечують в сучасних умовах необхідний рівень безпеки, такі як Telnet і протокол передачі файлів FTP. Для шифрування бездротового зв'язку широко використовуються сучасні протоколи WPA/WPA2. Також використовується досить старий протокол WEP, який поступається з безпеки. ITU-T G.hn та інші провідні

комунікації шифруються за допомогою AES, а автентифікацію та обмін ключами в них забезпечує X.1035. Для шифрування електронної пошти використовують такі програми як PGP та GnuPG.

Міжмережеві екрани (МСЕ). Рішення, які забезпечують фільтрацію та блокування небажаного трафіку, контролюють доступ до мережі. Розрізняють такі види фаєрволів, як мережеві та хост-сервери. Мережеві фаєрволи розміщуються на шлюзових ПК LAN, WAN та в інтрамережах. Міжмережевий екран може бути виконаний у форматі програми, встановленої на звичайний комп'ютер або мати програмно-апаратне виконання. Програмно-апаратний фаєрвол - це спеціальний пристрій на базі операційної системи з встановленим МСЕ. Крім основних функцій, міжмережеві екрани пропонують низку додаткових рішень для внутрішньої мережі. Наприклад, виступають як сервер VPN або DHCP.

Віртуальні приватні мережі VPN (Virtual Private Network). Рішення, що використовує в межах загальнодоступної мережі приватну мережу для передачі та приймання даних, що дає ефективний захист підключених до мережі програм. За допомогою VPN забезпечується можливість віддаленого підключення до локальної мережі, створення спільної мережі головного офісу з філіями. Безпосередньо для користувачів VPN дає можливість приховувати розташування та захист дій, що виконуються в мережі.

Проксі-сервер. Виконує функцію шлюзу між комп'ютером та зовнішнім сервером. Запит, що надсилається користувачем на сервер, спочатку надходить на proxy і вже від імені надходить на сервер. Повернення відповіді здійснюється також із проходженням проміжної ланки - proxy. Перевагою є те, що кеш проксі-сервера доступний для всіх користувачів. Це підвищує зручність у роботі, оскільки ресурси, що найчастіше запитуються, знаходяться в кеші.

Рішення SIEM - системи моніторингу та управління інформаційною безпекою. Спеціалізоване ПЗ, яке перебирає функцію управління безпекою даних. SIEM забезпечує збирання відомостей про події з усіх джерел, що підтримують безпеку, у тому числі від антивірусного ПЗ, IPS, фаєрволів, а також

від операційних систем тощо. Також SIEM виконує аналіз зібраних даних та забезпечує їх централізоване зберігання в журналі подій. На підставі аналізу даних система виявляє можливі збої, атаки хакерів, інші відхилення та можливі інформаційні загрози. Як було зазначено вище, однією з серйозних загроз від персоналу є загроза витоку службової інформації. Подібні інциденти часто на слуху через широке коло порушених осіб. Витоки конфіденційної інформації полегшуються існуванням численних каналів, доступних майже кожному співробітнику організації та організацій, що зв'язують корпоративні мережі, з Інтернетом (до них належать месенджери, електронна пошта), поширенням знімних носіїв інформації великого обсягу, що легко підключаються майже до будь-якого комп'ютера, а також поширенням бездротових мереж. [17]

Найкращі практики щодо запобігання витоку даних

1. Регулярно оцінюйте ризики.

Можливо, у вашій організації існує стратегія кібербезпеки. Однак це не робить ваші дані повністю безпечними, тому що хакери постійно винаходять нові методи виявлення будь-яких вразливостей в системі. Отже, необхідно проводити регулярні оцінки вразливостей та аудити кібербезпеки, щоб переконатися, що чинні політики є достатньо надійними, щоб тримати зловмисників під замком.

2. Інформованість працівників

Співробітники відіграють величезну роль у запобіганні витоку даних. Коли персонал не поінформований про передові методи запобігання витоку даних, вони, швидше за все, стануть найсерйознішою вразливістю безпеки даних. Поінформованість співробітників гарантує, що вони можуть оцінити кібербезпеку та знати, як виявляти будь-які загрози безпеці системи, а також що робити у разі спроби атаки.

3. Використовуйте оновлене програмне забезпечення

Необхідно регулярно оновлювати операційні системи та прикладне програмне забезпечення, щоб зменшити вразливі місця, які можуть використовувати хакери для атак. Переконайтеся, що ви встановлюєте

виправлення будь-коли, коли вони доступні. Застаріле програмне забезпечення без виправлень робить вашу мережу вразливою для атак.

4. Отримайте сертифікат SSL

Більшість хакерів одержують доступ до конфіденційної інформації, порушуючи з'єднання клієнт-сервер. З сертифікатом SSL інформація, що надсилається мережею, зашифровується, що робить її нечитаною для будь-кого, крім законних одержувачів.

Сертифікати SSL забезпечують шифрування та цілісність даних, гарантуючи, що дані не будуть пошкоджені. Крім того, вони аутентифікують дані, гарантуючи, що тільки люди з належною аутентифікацією можуть отримати доступ до даних. Сертифікати SSL доступні у різних типах та на різних рівнях перевірки.

Якщо вам потрібно захистити окремі домени разом з піддоменами, рекомендується купити Comodo Positive SSL Wildcard. Це економічний і зручний спосіб для компаній швидко захистити окремий домен і необмежену кількість піддоменів за допомогою одного сертифіката.

5. Складіть план реагування на порушення

Життєво важливо мати структуру, яку можна використовувати відновлення після спроби злому. Ця стратегія допомагає керувати збитками від атаки та відновлювати суспільну довіру, якщо атака все ж таки відбудеться.

6. Регулярно виконуйте резервне копіювання

Жодна система не може похвалитися повною несприйнятливістю до різноманітних кібератаки або втрати даних. Втрата даних - досить поширене явище, яке може завдати шкоди компанії чи приватній особі. Правильна стратегія резервного копіювання допомагає зменшити збитки від витоку даних. Коли у вас є резервні копії, легко відновити операції, і це заощадить вам багато грошей у разі атаки програми здирника. Резервне копіювання даних слід виконувати регулярно. Чим конфіденційні дані, тим частіше необхідно їх резервне копіювання. Ви можете автоматизувати процес резервного копіювання, щоб забезпечити швидке резервне копіювання важливих даних. Крім того, ваша

стратегія резервного копіювання має бути надмірною. Таким чином, у вас завжди буде робоча копія, якщо одна із резервних копій вийде з ладу.

Нарешті, переконайтеся, що процес відновлення відбувається швидко і плавно, щоб ви могли повернутися до звичайних операцій якнайшвидше після кібератаки. [18]

В останнє десятиліття швидко сформувався окремий сегмент ринку відповідних спеціалізованих захисних заходів – систем захисту від витоків, DLP. Дані кошти спрямовані на виявлення та блокування ситуацій витоку конфіденційної інформації каналами зв'язку. Учасники ринку активно просувають такі кошти під прапором «боротьби» з інсайдерами, із внутрішніми загрозами ІБ. При тому що прогрес у розвитку подібних технічних засобів можна оцінити лише позитивно, слід пам'ятати, що тільки комплексний підхід дозволить розв'язувати проблему. Загрози від персоналу не вичерпуються одними лише витоками, інші загрози є не менш небезпечними та рідкісними. Водночас, ефективне застосування DLP вимагає серйозних організаційних політик у сфері класифікації інформації та у сфері управління оборотом службової інформації.

Список DLP-систем

Відповідно до огляду «Російський ринок DLP-систем 2021. Проблеми та рішення» від ICT-Online.ru основні гравці та рішення на російському ринку DLP:

- DeviceLock DLP
- Falcongaze SecureTower
- Infowatch Traffic Monitor DLP
- Zecurion DLP
- Ростелеком Solar Dozor DLP
- SearchInform DLP
- Гарда Підприємство
- Kaspersky DLP

Закордонні рішення:

- Symantec DLP

- Forcepoint DLP
- McAfee DLP
- Sophos Endpoint Protection
- Digital Guardian

Порівняння DLP – систем.

У процесі вибору між тим чи іншим рішенням неминуче виникають питання. Чим принципово відрізняються між собою різні рішення? На що орієнтуватись при виборі DLP-системи? Як вибрати найбільш відповідне рішення для вашої компанії?

Відповідь на ці питання криється у завданнях, які планується вирішувати за допомогою DLP-системи. На жаль, універсального рішення, яке підходить будь-якій компанії, сьогодні немає. Саме тому важливо розуміти, чим один продукт відрізняється від іншого. [19]

Нижче було проведено порівняння декількох популярних DLP – систем за функціоналом, режимом роботи та термінами впровадження.

Таблиця 3.1.

Загальна інформація

Назва	SearchInform	InfoWatch EndPoint Security	Solar Dozor	Symantec Data Loss Prevention
Порівнювані версії	Endpoint Sniffer 5.0.16.31, Network Sniffer 5.0.342.0, AlertCenter 4.0.57.4, SearchInformClient 4.5.9.85, DataCenter 2.0.0.4.	InfoWatch Traffic Monitor Enterprise 5.1	Дозор-Джет 5.01	Symantec Data Loss Prevention 12.0.1
Сертифікати	ФСТЕК. Сертифікат відповідності №2851 від 8.05.2013 р. ДСТЗІ України. Сертифікат відповідності №448 від 21.06.2013 р.	ФСТЕК. Сертифікат відповідності ПДВ 4 та ІСПДн 1, Газпромсерт, Акредитація ЦП, Експертний висновок ОАЦ	ФСТЕК ОУД 3+ 1Г НДВ 4 та ІСПДн 1, Газпромсерт	ФСТЕК. Сертифікат відповідності № 2602 від 22.03.2012 ТУ+ПДВ за 4 рівнем контролю

Терміни впровадження	Від 1 робочого дня залежно від попередньої підготовки та кількості робочих станцій	Від кількох годин до 1 робочого тижня залежно від розміру компанії та завдань, що вирішуються клієнтом	Від кількох днів до 1 робочого тижня	Від 1 робочого дня в залежності від масштабу застосування
Інтерфейс	Російська, англійська (опційно: Польська, Литовська, Латиська)	Англійська, Російська, Білоруська, Українська	Російська, англійська	Російська, Англійська, Японська, Китайська, Бразильська, Французька та інші
Цільовий сегмент	Великі корпоративні клієнти, середній та малий бізнес	Великі корпоративні клієнти, держсектор. Для SMB компаній рішення InfoWatch Traffic Monitor Standard	Великі корпоративні клієнти, держсектор	Малий бізнес, середній та великий бізнес від 50 до 100 тис. робочих місць

Таблиця 3.2.

Режими роботи

	SearchInform	InfoWatch EndPoint Security	Solar Dozor	Symantec Data Loss Prevention
Робота в режимі моніторингу	Так	Так	Так	Так
Робота в режимі блокування	Так	Так	Так	Так
Робота системи поза мережею компанії	Так	Так	Так	Так

Таблиця 3.3.

Контроль користувачів

	SearchInform	InfoWatch EndPoint Security	Solar Dozor	Symantec Data Loss Prevention
Знімки екрану	Так	Так	Так, з можливістю вибору режиму	Ні, але можна вимкнути можливість робити знімки
Перегляд робочого столу в режимі реального часу	Так	Ні	Ні	Ні
Запис звуку через мікрофон ноутбука або підключену гарнітуру	Так	Ні	Ні	Ні
Протоколювання часу роботи у додатках	Так	Ні	Ні	Ні
Контроль запуску додатків	Так	Так	Так	Так

Таблиця 3.4.

Пошук конфіденційної інформації у мережі підприємства

	SearchInform	InfoWatch EndPoint Security	Solar Dozor	Symantec Data Loss Prevention
Сканування робочих станцій	Так	Так	Так	Так
Сканування загальних мережевих сховищ	Так	Так	Так	Так
Сканування сховищ Microsoft SharePoint	Так	Так	Так	Так
Створення тіньових копій знайдених конф. документів	Так	Так	Так	Так
Запуск завдань вручну або за розкладом	Вручну, за розкладом	Вручну, за розкладом	Вручну, за розкладом	Вручну, за розкладом
Видалення або переміщення конфіденційних даних до карантину	Ні	Ні	Ні	Так

Це лише один зі інструментів, який поодинці не дозволить вирішити завдання в загалом. Крім того, такі засоби вимагають ретельного налаштування з періодичною актуалізацією налаштувань.

Варто відзначити важливий момент. Використання DLP коли вже очевидно, що хтось зливає інформацію – неефективно. Співробітникам відділу безпеки потрібен час, щоб зібрати базу підозрілих дій. Тому встановлювати DLP-систему потрібно відразу, як тільки дозволяють фінансові можливості, а не чекати, поки інсайдер продасть вашу інформацію конкурентам. [20]

3.2. Рекомендації щодо вибору оптимального комплексного рішення для організації захисту підприємства від внутрішніх загроз

Комплексна система захисту інформації (КСЗІ)

КСЗІ – сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу.[21]

КСЗІ є глобальною концепцією безпеки та основою для безпеки інфраструктури підприємства загалом. [22]

Алгоритм побудови КСЗІ

1. Аудит
    - Аналіз поточного стану інформаційної безпеки;
2. Розробка технічного завдання
    - Аналіз уразливостей інформаційної системи;
    - Визначення вимог до системи захисту;
    - Розробка інформаційної моделі КСЗІ;
3. Визначення технічного рішення
    - Визначення детального переліку обладнання, програмного забезпечення та утримання робіт;
    - Опис технічного рішення (робочий проєкт);
    - Визначення вартості;
4. Реалізація КСЗІ

- Побудова повного комплексу засобів захисту;
- Тестування КСЗІ;

5. Експертиза
    - Отримання експертного висновку (атестата);
6. Експлуатація
    - Підтримка актуальності КСЗІ протягом життєвого циклу.

Комплексний підхід до захисту в першу чергу виражається в кореляції подій безпеки та інтеграції різних механізмів захисту між собою. Сучасна система захисту повинна будуватися не на розрізнених засобах захисту, здатних працювати тільки у своїй вузькій сфері, а на комплексних продуктах, які вміють зіставляти між собою різні події та дозволяють виробляти комплексну реакцію в залежності від загальної ситуації. [23]

Не можна також забувати, що забезпечення ІБ - безперервний процес. Поки існує сама інформація, що вимагає захисту, система менеджменту ІБ (СМІБ) повинна ґрунтуватися на відомій моделі PDCA (Plan-Do-Act-Control, плануй - роби - перевіряй - впливай). [24]

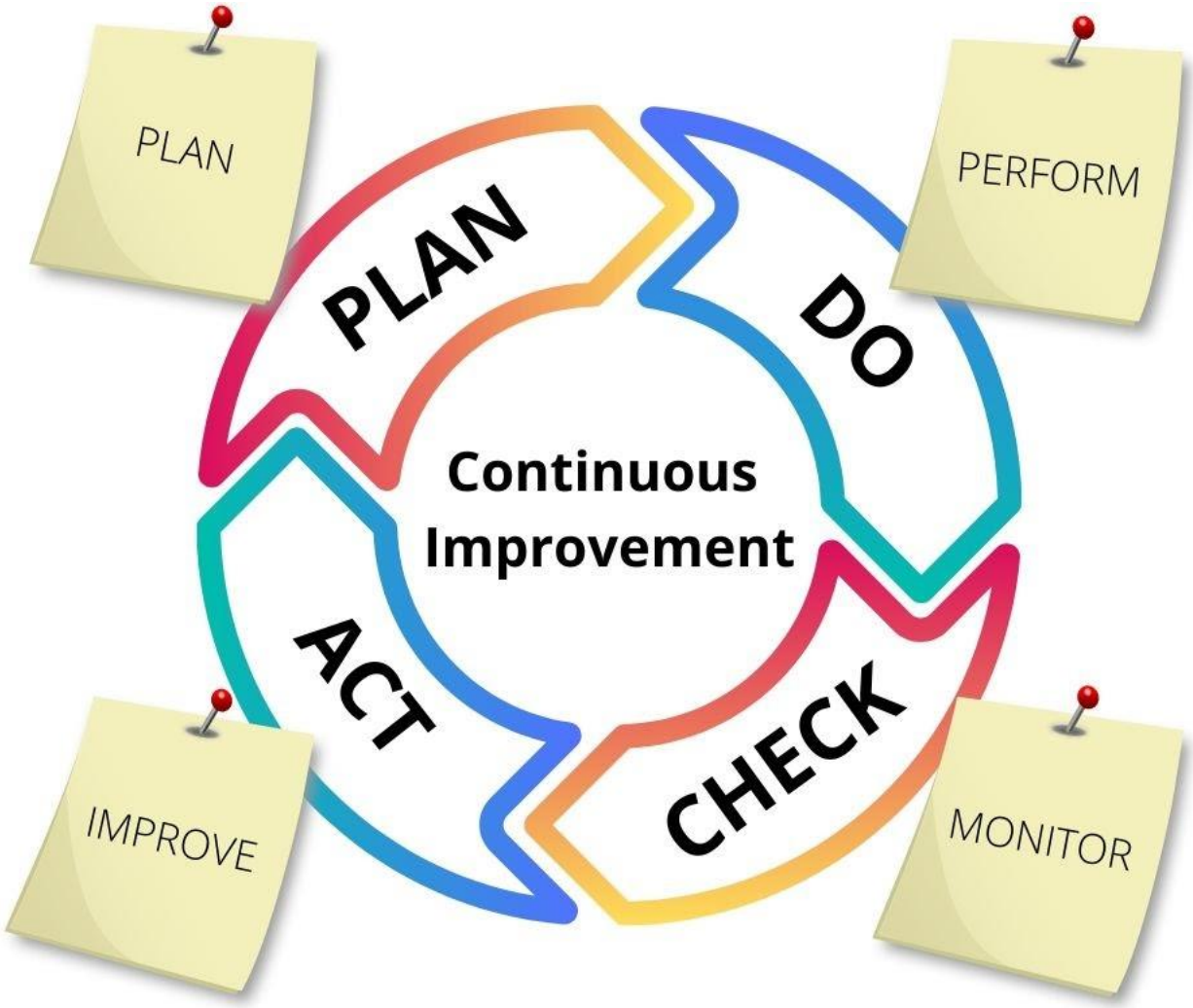

Рис. 3.1. Цикл Шухарта-Демінга (PDCA).

При захисті конфіденційної інформації хорошою практикою є використання комплексного підходу - тобто комбінація організаційних і технічних заходів, наприклад, таких як:

- Проведення аудиту процесів обробки конфіденційної інформації та інфраструктури, залучений в таких процесах, на відповідність вимогам законодавства, галузевим стандартам і внутрішньої документації з інформаційної безпеки;
- Розробка / доопрацювання комплекту організаційно-розпорядчої документації, яка описує цілі, вимоги й процедури щодо захисту інформації;
- Проєктування і впровадження системи захисту інформації, яка може складатися з наступних модулів: ідентифікація, аутентифікація, авторизація користувачів (SSO, OTP, біометрія), управління обліковими записами (IdM),

захист кінцевого обладнання (антивіруси, апаратні замки), мережева безпека (міжмережеві екрани, VPN, пісочниці), інфраструктура відкритих ключів (УЦ, HSM), захист віртуальних середовищ (VMsec), управління інцидентами (SIEM, IRP), патч-менеджмент, захист від витоків (DLP), безпека мобільних пристроїв (MdM), захист доступу в інтернет (WAF, proxy).

- Систематичне навчання співробітників процедурам щодо захисту інформації: в тому числі політиці «чистого стола» та правилам знищення паперових носіїв інформації;
- Планові та позапланові перевірки: тести на проникнення, моделювання сценаріїв інцидентів, використання соціальної інженерії. [25]

Комплексний підхід виражається у виробленні належних політик інформаційної безпеки, введенням чіткої організаційної структури відповідальних за інформаційну безпеку співробітників, контроль документообігу, контролю та моніторингу користувачів, введення просунутих механізмів аутентифікації для доступу до інформації різного ступеня важливості.

До організаційних методик належать:

- створення концепції інформаційної безпеки;
- ретельний добір працівників на відповідальні посади;
- складання посадових інструкцій та навчання правилам ІБ усіх працівників;
- організація надійного пропускного режиму на територію підприємства;
- контроль роботи працівників, які мають доступ до секретних відомостей;
- забезпечення надійної фізичної охорони підприємства;
- організація автоматизованої обробки секретних відомостей;
- ретельна розробка планів дій щодо виявлення спроб незаконного доступу, копіювання, зміни чи видалення інформаційних ресурсів.

Поряд з організаційними методиками вдаються до технічного захисту інформації. Вона є комплексом технічних засобів, вибір яких безпосередньо

залежить від типу та кількості об'єктів захисту. Інженерно-технічний захист включає застосування захищених підключень, засобів шифрування. Додатково часто встановлюють системи охоронно-пожежної сигналізації.[26]

Основними методами захисту є:

1. Антивірусний захист. Це спеціалізоване програмне забезпечення для виявлення та знищення вірусів. Серед найпоширеніших антивірусних програм виділяються Kaspersky та Dr.Web. Найчастіше одна організація паралельно використовує кілька антивірусів.

2. Шифрування (криптографічні засоби). Це процес перетворення відкритих даних на закриті за допомогою секретного елемента - ключа шифрування. Шифрування гарантує стабільний захист інформації.

3. Захист інформації в мережі (використання Virtual Private Network). Використання приватної мережі передачі даних включає кілька умов: тунелювання, шифрування й аутентифікація. Тунелювання гарантує передачу даних між вузлами користувачів таким чином, що з боку програмного забезпечення, вони будуть виглядати підключеними до однієї мережі. Пакет даних проходить крізь різні вузли мережі. Для їх захисту застосовують електронний цифровий підпис. Це блок інформаційних ресурсів, який передається поряд із пакетом даних і формується згідно з криптографічним алгоритмом. Він є винятковим для вмісту пакета та ключа електронного цифрового підпису відправника. Блок інформаційних ресурсів дає можливість виконати розпізнавання даних одержувачем, який знає ключ електронного підпису відправника (аутентифікація). Це гарантує захищеність пакета даних.

4. Proxy Servers. Звертання з локальної мережі до глобальної мережі здійснюються за допомогою спеціальних серверів. Однак цей спосіб не дає 100% захисту проти серйозних загроз (зокрема вірусів).

5. Міжмережеві екрани (брандмауери). Брандмауери забезпечують поділ мереж та запобігають порушенням встановлених правил безпеки користувачами. Контроль за передачею даних відбувається шляхом фільтрації трафіку;

Ступінь такого захисту залежить від об'єктивних потреб організації в захисті інформації. Далеко не всім об'єктам потрібна дорога DLP-система, що дає непогані результати по захисту даних підприємства від витоків, але вимагає складної процедури впровадження і перегляду поточних механізмів документообігу. Оптимальним вибором для більшості компаній стане введення функціоналу захисту від витоків даних, контроль документообігу і моніторинг дій користувачів локальної мережі організації. Таке рішення є недорогим, простим в розгортанні й експлуатації, але досить ефективним інструментом інформаційної безпеки. [27]

До технічних заходів можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів на встановлення резервних систем електроживлення, оснащення замків, установку сигналізації та ін. [28]

Фахівці виділяють такі основні напрямки технічного захисту комп'ютерної системи:

- захист інформаційних ресурсів від несанкціонованого доступу та використання; використовуються засоби контролю завантаження програмного забезпечення, а також методи парольного захисту при вході до системи;
- захист від витоку побічними каналами електромагнітних випромінювань і наведень за допомогою екранування апаратури, приміщень, застосуванням генераторів для маскування шумів;
- захист інформації в каналах зв'язку та вузлах комутації
- використовуються процедури автентифікації абонентів та повідомлень, шифрування та спеціальних протоколів зв'язку;
- захист юридичної значущості електронних документів — у разі необхідності передачі документів (платіжних доручень, контрактів) по комп'ютерних мережах
- для визначення істинності відправника документ доповнюється електронним цифровим підписом - спеціальною міткою, нерозривною, логічно

пов'язаною з текстом та формованою за допомогою секретного криптографічного ключа;

- захист автоматизованих систем від комп'ютерних вірусів та незаконної модифікації.

Самі технічні заходи захисту можна розділити на:

- Засоби апаратного захисту, що включають засоби захисту кабельної системи, систем електроживлення і т.д.
- програмні засоби захисту, зокрема: криптографія, антивірусні програми, системи розмежування повноважень, засоби контролю доступу тощо;
- заходи щодо підготовки та навчання персоналу, організації тестування та прийняття в експлуатацію програм, контролю доступу до приміщень тощо. [29]

Слід зазначити, що такий поділ досить умовний, оскільки сучасні технології розвиваються у напрямку поєднання програмних та апаратних засобів захисту. Найбільшого поширення таких програмно-апаратних засобів набули, зокрема, у сфері контролю доступу, захисту від вірусів тощо.

Під апаратними засобами маються на увазі спеціальні засоби, що безпосередньо входять в склад технічного забезпечення і виконують функції захисту як самостійно, так і в комплексі з іншими засобами, наприклад, з програмними. [30]

Програмними називаються засоби захисту даних, що функціонують у складі програмного забезпечення. З них можна виділити та докладніше розглянути наступні:

- засоби архівації даних;
- міжмережеве екранування;
- антивірусні програми;
- криптографічні засоби;
- засоби ідентифікації та аутентифікації користувачів (розмежування доступу);
- захист від витоків інформації;

- протоколювання та аудит.

Комплексна система захисту інформації на підприємстві або в організації передбачає забезпечення безпеки критичних процесів, реалізовану відповідно до вимог перевірчих органів (регуляторів). [31]

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

Сьогодні інформаційні технології є важливим складником будь-якої сучасної організації. Говорячи образно, інформаційні технології – це серце підприємства, яке підтримує працездатність бізнесу та підвищує його ефективність та конкурентоспроможність в умовах сучасної, жорсткої конкуренції.

Стає очевидним, що велика кількість стратегічних, конфіденційних та персональних даних є важливим інформаційним активом підприємства, і наслідки витоку цієї інформації позначаться на ефективності діяльності організації.

Автор вважає, що найбільшого поширення сьогодні набули програмні засоби захисту інформації. Вони повністю відповідають вимогам ефективності та актуальності, регулярно оновлюються, ефективно реагуючи на актуальні загрози.

Було проведено аналіз й порівняльна характеристика в вигляді таблиці можливостей та функціоналу найпопулярніших DLP – систем.

Для захисту даних у сучасних мережах використовується широкий спектр спеціалізованого програмного забезпечення. Такого як антивірусне ПЗ, хмарні антивіруси, DLP - системи, системи криптографії, міжмережеві екрани, VPN, проксі сервери та рішення SIEM.

Автор рекомендує використовувати комплексний підхід який виражається у виробленні належних політик інформаційної безпеки, введенням чіткої організаційної структури відповідальних за інформаційну безпеку

співробітників, контроль документообігу, контролю та моніторингу користувачів, введення просунутих механізмів аутентифікації для доступу до інформації різного ступеня важливості, які детально розписав у третьому розділі своєї роботи.

ВИСНОВКИ

В ході виконання дипломної роботи були запропоновані процеси й методи для забезпечення захисту інформаційних систем підприємства. В результаті роботи були розглянуті особливості внутрішніх порушень ІБ.

Було визначено, що інвестиції в кібербезпеку на закордонному ринку зростають досить гарними темпами, також визначили, що попит на фахівців з організації інформаційної безпеки росте, через відсутність добре підготовлених фахівців.

Автор визначив, що для захисту даних у сучасних мережах використовується широкий спектр спеціалізованого програмного забезпечення.

Таке яке може складатися з наступних модулів: ідентифікація, аутентифікація, авторизація користувачів (SSO, OTP, біометрія), управління обліковими записами (IdM), захист кінцевого обладнання (антивіруси, апаратні замки), мережева безпека (міжмережеві екрани, VPN, пісочниці), інфраструктура відкритих ключів (УЦ, HSM), захист віртуальних середовищ (VMsec), управління інцидентами (SIEM, IRP), патч-менеджмент, захист від витоків (DLP), безпека мобільних пристроїв (MdM), захист доступу в інтернет (WAF, proxy).

З переходом підприємств на дистанційну роботу, методи захисту повинні удосконалюватись й тримати направлення на захист хмарних сервісів.

Було наведено приклади, реальних випадків витоків даних і методи бородьби з ними.

Дослідження показує, що більшість витоків відбувається з особистої вигоди працівників які мають доступ до інформаційних систем підприємства.

Автор вважає, що більшість внутрішніх порушень інформаційної безпеки відбувається із за ображених або некомпетентних кадрів які працюють з інформаційними системами компанії.

Крім того, визначенно, що внутрішньому порушнику заздалегідь відомо, яку інформацію можна використовувати для вилучення особистої вигоди.

Тому використання комплексних систем захисту інформації просто вкрай необхідно.

КСЗІ є глобальною концепцією безпеки та основою для безпеки інфраструктури підприємства загалом.

Автором було надано рекомендації щодо вибору оптимального комплексного підходу для захисту інформаційних активів підприємства.

Оптимальним вибором для більшості компаній стане введення функціоналу захисту від витоків даних, контроль документообігу і моніторинг дій користувачів локальної мережі організації. Таке рішення є недорогим, простим в розгортанні й експлуатації, але досить ефективним інструментом інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Валерий Васильев «Внутренние и внешние ИБ-угрозы: есть ли смысл в их разделении?» URL: https://www.itweek.ru/security/article/detail.php?ID=178063 (дата звернення: 12.10.2021).

2. Solar Security – «Какие организации чаще других подвержены внутренним нарушениям корпоративной безопасности» URL: https://rt-solar.ru/analytics/reports/ (дата звернення: 12.10.2021).

3. Единый Стандарт – «PDCA простыми словами» URL:https://1cert.ru/stati/pdca-prostymi-slovam (дата звернення: 12.10.2021).

4. StaffCop – «Общие сведения об информационной безопасности» URL: https://www.staffcop.ru/blog/obshchie-svedeniya-ob-informatsionnoj-bezopasnosti (дата звернення: 13.10.2021).

5. InfoProtect – «Модель нарушителя информационой безопасности» URL: http://infoprotect.net/varia/modelyy_narushitelya_informacionnoy_bezopasnosti (дата звернення: 13.10.2021).

6. VS.RU – «Успешные методы внутренней борьбы с утечками информации в вашем офисе» URL: https://vc.ru/office/136394-uspeshnye-metody-vnutrenney-borby-s-utechkami-informacii-v-vashem-ofise (дата звернення: 14.10.2021).

7. Statista – «Revenue of information technology (IT) security market in Ukraine from 2018 to 2020» URL: https://www.statista.com/statistics/1269725/it-security-market-revenue-by-segment-ukraine/ (дата звернення: 14.10.2021).

8. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 1999. – № 14 : Міжнародні відносини. – С. 46-48.

9. ChannelForIt – «Рынок информационной безопасности в Украине» URL: https://channel4it.com/publications/Rynok-informacionnoy-bezopasnosti-v-Ukraine-vremya-deystvovat-21041.html (дата звернення: 26.10.2021).

10. Datamation – «Cybersecurity Market 2021» URL: https://www.datamation.com/security/cybersecurity-market/#companies (дата звернення: 26.10.2021).

11. Stefanini – «Top 9 Cybersecurity Trends to Adapt in 2022» URL: https://stefanini.com/en/trends/articles/top-9-cybersecurity-trends-to-adapt-in-2022 (дата звернення: 27.10.2021).

12. Gartner – «Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021» URL: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem (дата звернення: 27.10.2021).

13. Crunchbase – «Report: The Rise Of Global Cybersecurity Venture Funding» URL: https://about.crunchbase.com/cybersecurity-research-report-2021/ (дата звернення: 28.10.2021).

14. Березюк, Л. П. Организационное обеспечение информационной безопасности : навч. посібник / Л. П. Березюк. – Хабаровськ : ДВГУПС, 2008. – 188 с.

15. Anti-Malware – «5 реальных примеров внутренних атак, которые можно было предотвратить» URL: https://www.anti-malware.ru/analytics/Threats_Analysis/5-real-examples-of-internal-attacks#part21 (дата звернення: 28.10.2021).

16. Ekran – «5 Real-Life Examples of Breaches Caused by Insider Threat» URL: https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches (дата звернення: 29.10.2021).

17. SecurityLab – «13 трендов рынка кибербезопасности и защиты информации 2019-2020» URL: https://www.securitylab.ru/blog/company/infosecurity/345651.php (дата звернення: 29.10.2021).

18. DataMI – «19 случаев масштабной утечки данных» URL: https://datami.ua/ru/19-sluchaev-masshtabnoj-utechki-dannyh/ (дата звернення: 30.10.2021).

19. SearchInform – «СРАВНЕНИЕ DLP-СИСТЕМ» URL https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/kak-vybrat-dlp-sistemu/sravnenie-dlp-sistem/ (дата звернення: 31.10.2021).

20. Stefanini – «Top 6 Best Practices for Preventing a Data Breach» URL: https://stefanini.com/en/trends/articles/top-6-best-practices-for-preventing-a-data-breach (дата звернення: 31.10.2021).

21. ВалТек – «Системи забезпечення інформаційної безпеки» URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review (дата звернення: 30.10.2021).

22. IntegritySystems – «Захист від витоку інформації» URL http://integritysys.com.ua/security/dlp/ (дата звернення: 01.11.2021).

23. Ленков С.В., Перегудов А.Д., Хорошко В.А. Методы и средства защиты информации – К.: Арий, 2008. – Том I. Несанкционированное получение информации. – 464с.

24. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с

25. Epam – «Комплексный подход к организации системы защиты информации на предприятии: основные вопросы и технологии» URL: https://www.epam-group.ru/about/newsroom/in-the-news/2009/kompleksnyy-podhod-k-organizacii-sistemy-zaschity-informacii-na-predpriyatii-osnovnye-voprosy-i-tehnologii (дата звернення: 09.11.2021).

26. UH – «Комплексная система защиты информации» URL: https://uh.ua/solutions-services/kszi.html (дата звернення: 09.11.2021).

27. Gov – «Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет» URL: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internetl (дата звернення: 10.11.2021).

28. Борсуковский, Ю. Подходы и решения : Информационная безопасность / Ю. Борсуковский // Мир денег. – 2001. – № 5. – С. 41-42.

29. Щербина, В. М. Інформаційне забезпечення економічної безпеки підприємств та установ / В. М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220-225.

30. Игнатьев, В. А. Информационная безопасность современного коммерческого предприятия: монографія / В. А. Игнатьев. – Старий Оскол : ООО «ТНТ», 2005. – 448 с.

31. CrossTehnologies – «СОЗДАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ» URL: https://crosstech.su/solutions/sozdanie-kompleksnoy-sistemy-zashchity-informatsii/ (дата звернення: 10.11.2021).

32. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.

33. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.

34. К. Мандиа, К. Просис. Защита от вторжений. Расследование компьютерных преступлений.– М., 2005.

35. Луцкер А. Авторское право в цифровых технологиях и СМИ. – М., 2005.

36. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: Автореф. дис. ... канд. юрид. наук: 12.00.08 / НАН України; Іа-т держави і права ім. В.М. Корецького. — К., 2003.

37. Брижко В.М., Гальченко О.М., Цимбалюк В.С. і ін. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. — К.: Інтеграл, 2002.

38. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. —- М.: Академический Проект; Фонд "Мир", 2003.

39. Василъченко 3. М. Структурні диспропорції у розвитку банківської системи України // Фінанси України. - 2005.

40. Віхорсв С. В., Кобцев Р. Ю. Як дізнатися - звідки напасти або звідки виходить загроза безпеці інформації // Захист інформації. Конфідент. – 2002

41. Вольоводз А. Г. Проект Європейської конвенції про кіберзлочини // Захист інформації. Конфідент -2001

42. Живко М. О. Захист інформації в системі економічної безпеки та підприємства /' Регіональне і місцеве самоврядування в нових умовах: партійна публічна адміністрація і безпосередня демократія: Мат-ли НІ укр.-польськ. наук.- практ. конф. (Львів, 2-4 березня 2006р.). - Л., 2006

43. Зегжда Д. П., Івашко А. М. Основы безопасности информационных систем.- М.: Гаряча лінія - Телеком, 2000.

44. Зубок М., Ніколаєва Л. Організаційно-правові основи безпеки банківської діяльності в Україні. - К.: Істина, 2000.

45. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: Авторсф. канд. юр. наук: 12.00.07/Нац. акад. внутр. справ України.

46. Організаційно-правові основи захисту інформації з обмеженим доступом: Навч. посібник / А. Б.Стоцький, А. М. Гуз, А. І. Марущак та ін.; За заг. ред. В. С. Сідака - К.: Вид-во Європ. ун-ту, 2006

47. Пархоменко П. И., Яковлев С. А., Пархоменко Н. Г. Правовые аспекты проблем обеспечения информационной безопасности: - Мат-ли V Междунар. науч.-практ. конф. "Інформационная безопасность".-Таганрог: ТРТУ, 2003.

48. Агафонов Г. Г., Буришев С. А., Прохоров С. Л. Концепции безопасности. / - К.: А-ДЕПТ, 2005.-Кн. 2.

49. Браіловський М. М., Дорошко В. О., Чирков Д. В., Шелест М. Е. Захист економічної інформації: Навч. посібник / За ред. проф. В. О. Хорошка: - К.: НАУ, 2002

50. Бруксбенк Д., Уилсон Дж. Руководство по безопасности: Пер. с англ. - М.: ЮНИТИ-ДАНА, 2003.

51. Про концепцію національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28.

52. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. Москва: Энергоатомиздат, 1994. 400 с.

53. Головань С.М. Базові вимоги до побудови моделі загроз інформаційних систем. Інформаційна безпека. 2009. №1. С.17-25.

54. Голубєв В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів. Запоріжжя, 1998. 144 с.

55. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Част. 3. Методи керування захистом інформаційних технологій. Чинний від 2004-01-01.

56. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие. Москва: Логос; ПБОЮЛ Н.А. Егоров, 2001. 264 с.

57. Ленков С.В., Перегудов А.Д., Хорошко В.А. Методы и средства защиты информации. Киев: Арий, 2008. Том I. Несанкционированное получение информации. 464 с.

58. Ленков С.В., Перегудов А.Д., Хорошко В.А. Методы и средства защиты информации. Киев: Арий, 2008. Том II. Информационная безопасность. 344 с.

59. Міжнародний стандарт ISO/IEC 17799:2005 Information technology Securitytechniques – Code of practice for information security management. 113

60. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

61. Ткачук Т. Шляхи запобігання та протидії промисловому шпигунству. Бизнес и безопасность. 2007. №3. С.7.

62. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: підручник. Київ: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. 716 с.