МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.5

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система захисту персональних даних на підприємстві

Виконавець: В.В. Дідан
Керівник: к.т.н., доцент С.В. Єгоров
Нормоконтролер: к.т.н., доцент С.В. Єгоров

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 20__ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Дідана Володимира Володимировича

1. Тема: *Система захисту персональних даних на підприємстві*
затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізувати існуючі системи захисту персональних даних; на основі проведеного аналізу визначити переваги та недоліки кожної з них; розробити свою систему захисту даних на підприємстві.
4. Зміст пояснювальної записки: аналіз існуючих систем захисту персональних даних; розробка системи аналізу та оцінки ризиків для даної системи; розробка методики захисту даних на підприємстві.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	15.04.2021	*Виконано*
2.	Аналіз літературних джерел	16.04.2021	*Виконано*
3.	Обґрунтування вибору рішення	17.04.2021	*Виконано*
4.	Збір інформації	18.04.2021 - 25.04.2021	*Виконано*
5.	Дослідження сучасних систем захисту та оцінка ризиків персональним даним	26.04.2021 - 02.05.2021	*Виконано*
6.	Розробка методики та структури системи захисту персональних даних	03.05.2021 - 10.05.2021	*Виконано*
7.	Дослідження апаратного та програмного захисту систем	11.05.2021 - 19.05.2021	*Виконано*
8.	Розробка системи захисту персональних даних	20.05.2021 - 28.05.2021	*Виконано*
9.	Перевірка на антиплагіат	04.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	09.06.2021	*Виконано*
11.	Оформлення презентації	30.05.2021	*Виконано*
12.	Отримання рецензій від рецензента	08.06.2021	*Виконано*

Здобувач вищої освіти В. Дідан

(підпис, дата)

Керівник дипломної роботи С. Єгоров

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальним обсягом робота складає 91 сторінку, має 4 рисунки, 4 таблиці та 5 додатків. Список використаних джерел містить 30 найменувань і займає 4 сторінки.

Метою дипломної роботи є створення системи захисту персональних даних.

В дипломній роботі розглянуті питання ризиків для систем захисту персональних даних, а також проаналізовані та запропоновані методи та основні напрями захисту.

Запропонована система може використовуватися у реальних практичних СЗІ. Створення нової, надійної системи захисту персональних даних, яка може використовуватися у будь-якій галузі, в якій є ризик нанесення шкоди та викрадення персональних даних.

Ключові слова: персональні дані, система захисту персональних даних, інформація, шкідливе програмне забезпечення, інформаційна система.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СЗ	– система захисту
ПД	– персональні дані
СЗПД	– система захисту персональних даних
ЗБПД	– загроза безпеки персональних даних
ІСПД	– інформаційна система персональних даних
ОС	– операційна система
СФЗ	– система фізичного захисту
ПЕОМ	– персональна електронна обчислювальна машина
ПЗП	– постійний запам’ятовуючий пристрій
ОЗП	– оперативний запам’ятовуючий пристрій
ЗІ	– захист інформації
НСД	– несанкціонована спроба доступу
ІС	– інформаційна система
ЦСК	– централізована система керування

ВСТУП

Актуальність теми. Сьогодні питання захисту персональних даних є особливо гострим для державних установ та організацій, які своєю діяльністю узагальнюють та використовують інформацію про особу. Відповідно Закону України «Про захист персональних даних», Закону «Про захист інформації в інформаційно-телекомунікаційних системах» та численних нормативних актів, така інформація повинна бути захищена від модифікації, несанкціонованого доступу та розповсюдження [13].

Проект захисту персональних даних передбачає необхідність усередині компанії усвідомлювати важливість захисту персональних даних, обґрунтовувати це всім зацікавленим сторонам, аналізувати ризики недотримання законодавчих вимог, визначати приблизну вартість та графік реалізації проекту, розрахувати його можливий вплив на поточну діяльність компанії та вибрати оптимальне рішення.

У тому випадку, якщо на момент аудиту компанія навіть не має вигляду роботи із захисту персональних даних, можна очікувати жорстких санкцій за невиконання вимог законодавства про персональні дані, основні з яких будучи:

• притягнути компанію або її керівника до адміністративної відповідальності;

• примусове призупинення або припинення обробки персональних даних у компанії;

• зупинення або анулювання ліцензій на основну діяльність компанії.

У будь-якому випадку, незалежно від ступеня санкцій, негативний результат аудиту підриває репутацію компанії і, як наслідок, викликає недовіру з боку клієнтів, партнерів, співробітників, що неминуче призводить до ротації клієнтів, викликає нервозність у роботі команди.

Метою дипломної роботи створення системи захисту персональних даних на підприємстві.

Для досягнення поставленої мети слід вирішити наступні завдання:

- ознайомитися з існуючими системами захисту даних;
- створити особисту систему захисту персональних даних;
- дослідити створену систему захисту на підприємстві.

Об’єкт дослідження: процес захисту персональних даних на підприємстві.

Предмет дослідження: апаратні та програмні системи захисту даних.

Методи дослідження: аналіз існуючих систем захисту.

Практична цінність. Набула подальшого розвитку система захисту персональних даних, що призвело до поліпшення захисту особистої інформації, завдяки тому, що було удосконалено методи програмного та апаратного захисту системи, а саме нові засоби авторизації/автентифікації, програми пошуку вірусів, а також програми криптографічного захисту та мережеві екрани. Дана система може бути використана у реальних практичних СЗ.

РОЗДІЛ 1. СУЧАСНІ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Поняття персональних даних.

Сьогодні людське життя неможливе без надання інформації про себе іншим членам суспільства, органам державної влади. Як зазначено в ст. 2 Закону України «Про інформацію» від 02.10.1992, кожен має право на інформацію, що передбачає можливість безкоштовного отримання, використання, поширення, зберігання та захисту інформації, необхідної для здійснення його прав, свобод і інтересів. Широке поширення і використання інформаційних технологій, глобальних інформаційних систем та автоматизованих баз даних значно спрощує реалізацію цього права громадянами. Але, незважаючи на всі переваги, є один серйозний недолік - великий ризик несанкціонованого втручання в особисте життя і зловживань «приватних» даних [2].

Таким чином, право на захист особистих даних є одним з основних прав людини. В Конституції України закріплено положення про те, що ніхто не може втручатися в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Забороняється збирати, зберігати, використовувати і поширювати конфіденційну інформацію про особу без її згоди, за винятком випадків, передбачених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (стаття 32) [3].

Першою проблемою, з якою стикалися менеджери персональних даних під час реєстрації у національному реєстрі баз персональних даних, було визначення того, яка інформація стосується персональних даних, а яка - ні.

Відповідно до ст. 11 Закону України «Про інформацію» від 02.10.1992 р. Інформація про особу (персональні дані) - це інформація або сукупність відомостей про особу, яку ідентифікують або яку можна конкретно ідентифікувати. Конфіденційна інформація стосовно особи включає, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, а також її адресу, дату та місце народження.

У поясненнях Міністерства юстиції "Деякі питання практичного застосування українського закону "Про захист персональних даних" від 21.12.2011. Вказується, що українське законодавство не встановило і не може встановити переліку інформації про фізична особа, яка є персональними даними, за можливість застосування норм закону до різних ситуацій, у тому числі при обробці персональних даних у (автоматизованих) базах даних та файлах персональних даних, які можуть виникнути в майбутньому внаслідок змін у технологічній, соціальній, економічної та інших сфер суспільного життя, визнаючи існування проблеми, він не відповів на питання, яка інформація дозволяє ідентифікувати особу [6].

Веб-сайт нової державної служби України з питань захисту персональних даних також не дає конкретної відповіді на це питання, лише припускає, що визначення терміну "персональні дані", подане в законі України "Про захист персональних даних", повністю відповідає визначенню зазначеного періоду, передбаченому Конвенцією Ради Європи про захист персональних даних. до Обробки персональних даних " [7].

Конституційний Суд України, даючи офіційне тлумачення частини першої та другої статті 32 Конституції України, вважає інформацію про особисте та сімейне життя людини (особисті дані, що стосуються її) інформацією або сукупністю інформації щодо особи, яку ідентифікували або яку можна конкретно ідентифікувати, а саме: громадянство, освіта, сімейний стан, релігійні переконання, стан здоров’я, матеріальне становище, адреса, дата та місце народження, місце проживання та перебування тощо, дані про особисті майнові та позашлюбні стосунки цієї особи з іншими особами, зокрема членами сім'ї, а також інформація про події та явища, що відбулися або відбуваються в побутовій, інтимній, товариській, професійній, діловій та інших сферах особи життя, винні дані про вправу с обов'язки особи, яка займає посаду, пов'язану з виконанням функцій держави або місцевого самоврядування. Ця інформація про особу та членів її родини є конфіденційною і може бути передана лише за їх

згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [8].

Слід також зазначити, що у багатьох країнах здійснюється поділ персональних даних на загальні персональні дані, що означає прізвище, ім'я, по батькові, вигадка, місце проживання, а також на вразливі персональні дані, які зокрема включають персональні дані із зазначенням расових, політичних, релігійних чи інших переконань, а також даних, що стосуються стану здоров'я або сексуальності, засуджень до кримінальних покарань. Цей розділ необхідний для встановлення спеціального режиму захисту вразливих персональних даних.

Надання персональних даних особою, як правило, пов’язане з її вступом у певні правовідносини (професійні, цивільні, економічні тощо). Водночас імплементація закону не завжди відповідає положенням інших нормативних актів.

Підставою права на використання персональних даних є згода суб'єкта персональних даних на обробку його персональних даних. Відповідно до ч. 2 ст. 11 Закону України «Про інформацію» від 02.10.1992 р не дозволяє збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, за винятком випадків, передбачених законом, і лише в інтересах національної безпеки, економічного добробуту. буття і права людини.

Як зазначено в п.1 ч.1 ст.11 закону підставою права на використання персональних даних є згода суб'єкта даних на їх обробку. Іншими словами, з одного боку, законодавець дає фізичній особі право дати згоду на використання його персональних даних, а з іншого - передбачає адміністративну та кримінальну відповідальність власника персональних даних за їх використання без це згоду.

Наприклад, відповідно до ст. 24 Кодексу законів про працю України при укладенні трудового договору громадянин повинен пред'явити паспорт або інший документ, що посвідчує особу, трудову книжку, а у випадках, передбачених законодавством, також документ про освіту (спеціальність, кваліфікацію), стані медичні та інші документи [9].

Ця проблема стає актуальною в іншому аспекті. В результаті посилення заходів відповідальності за порушення закону роботодавці почали активно вимагати від співробітників згоди на використання їх персональних даних, які вже були ефективно отримані в процесі прийому на роботу. Більшість співробітників підписують така угода «автоматично», але деякі категорично відмовляються. Тут знову виникає питання: що робити роботодавцю, щоб уникнути відповідальності в разі незаконної обробки персональних даних? На сьогоднішній день ми можемо розраховувати тільки на те, що Державна служба України щодо захисту персональних даних під час перевірки буде чуйно ставитися до ситуації [1].

Виходячи з вищесказаного, є кілька виходів із ситуації. У разі персональних даних, які особа повинна надати при укладенні певних правовідносин, відповідно до чинного законодавства, необхідно виходити з того, що запитується згода. Іншими словами, його не потрібно постачати окремо. При цьому за фізичною особою зберігаються всі права на свої персональні дані, передбачені законом. Це можна зробити, включивши в закон положення про випадки, коли згода суб'єкта даних не потрібно. Наприклад, обробка персональних даних співробітника для здійснення прав і обов'язків у сфері трудових відносин, впорядкування і сплата податків і зборів здійснюється без згоди співробітника.

Інший варіант - надати алгоритм дій для власника персональних даних у разі, якщо суб'єкт цих даних не дає згоди на їх використання.

Ще один приклад застосування закону в сфері цивільного права. Відповідно до ч. 1 ст. 633 ЦК України, договір, в якому сторона - підприємець взяла на себе зобов'язання здійснити продаж товарів, виконання робіт або надання послуг кожному, хто звернеться до нього (торгівля вроздріб, транспорт по громадський транспорт, послуги зв'язку, медичні послуги, готель, банківська справа та ін.). При цьому важливою гарантією прав споживачів є положення про те, що підприємець не може відмовитися від укладення державного договору, якщо у нього є можливість поставити споживачеві відповідні товари (роботи,

послуги). У разі необґрунтованої відмови підприємця від укладення державного договору він повинен відшкодувати збиток, заподіяний споживачеві такою відмовою (ч. 4 ст. 633 ЦК України) [1].

У цьому випадку відмова підприємця від надання послуги споживачеві через незгоду останнього на використання його персональних даних буде вважатися необґрунтованою.

Тому, на мій погляд, закон повинен у виняткових випадках передбачати можливість обробки персональних даних, необхідних для укладення та виконання договору, без згоди суб'єкта даних. Своєчасність таких змін обумовлена тим, що майже всі компанії мають таку персональну базу даних і тому зобов'язані її реєструвати. Це особливо актуально для юридичних осіб, що надають послуги населенню.

Персональні дані сторін трудового договору, під якими мається на увазі інформація про роботодавця і працівника, має важливе значення для кожного з них. При укладанні трудового договору працівник отримує інформацію про роботодавця, про місце його знаходження, характер майбутньої роботи. Велике значення знання персональних даних працівника має для роботодавця, який при укладанні трудового договору отримує інформацію про працівника, про його вік, професію, спеціалізації, кваліфікації, стан здоров'я, сімейний стан.

Після укладення трудового договору інформація про працівника необхідна роботодавцю для належного виконання його зобов'язань, що випливають не тільки з трудового, а й з цивільного, сімейного, адміністративного, інших галузей законодавства (наприклад, для утримання із заробітної плати податків, коштів на відшкодування шкоди, аліментів) , для надання працівникові пільг і переваг, наприклад, при перекладі на іншу роботу в зв'язку з хворобою, вагітністю, наявністю дітей.

Надаючи роботодавцю право отримувати об'ємну інформацію про персональні дані працівника, закон зобов'язує його вживати всіх заходів для запобігання несанкціонованому виходу цієї інформації з ведення роботодавця,

щоб персональні дані працівника не стали надбанням третіх осіб без його відома і згоди.

Коло інформації, що відноситься до персональних даних працівника, визначається роботодавцем з урахуванням умов, визначених трудовим законодавством стосовно того чи іншого виду трудового договору і трудової діяльності, а також з урахуванням характеру виконуваної роботи. Наприклад, спеціальна інформація буде потрібна роботодавцю для укладення з працівником трудового договору на виконання роботи, що вимагає спеціальних знань або допуску до державної таємниці.

1.2. Аналіз загроз для персональних даних.

Загрози безпеці - це певний набір умов або факторів впливу, що створюють небезпеку стосовно персональних даних, що полягає у ознайомленні несанкціонованих осіб із захищеними персональними даними, модифікації, знищенні, розповсюдженні, а також інших незаконних діях з персональними даними.

Джерелами загроз безпеці персональних даних можуть бути як внутрішні порушники, тобто їх власні працівники, так і зовнішні порушники, які використовують канали зв'язку, комп’ютерні мережі та Інтернет для реалізації загрози. Крім того, загрози безпеці можуть виникати при введенні в інформаційну систему шкідливих програм та вірусів.

Засобами реалізації загроз безпеці можуть бути несанкціонований доступ до інформації, витоки через технічні канали, а також особливий вплив на персональні дані або інформаційну систему.

Загроза несанкціонованого доступу до персональних даних, що обробляються в інформаційній системі, може бути вирішена за допомогою програмного та апаратного забезпечення та програмних засобів. У цьому випадку має місце порушення режиму конфіденційності персональних даних

шляхом їх незаконного копіювання та / або розповсюдження. Крім того, захищені персональні дані можуть бути змінені або знищені порушником, що також може призвести до значних наслідків. При реалізації загрози несанкціонованого доступу можуть бути створені ненормальні режими роботи операційного середовища або програмного забезпечення, які зловмисник може використовувати для викрадення інформації або впливу на неї звідти.

Реалізуючи загрозу безпеці, зловмисник може використовувати різні вразливі місця, включаючи недостатній рівень захисту, недосконаліть системного та прикладного програмного забезпечення, а також мережеві протоколи комунікації інформаційної системи.

Іншим видом загроз безпеці персональних даних є загрози, реалізовані за допомогою технічних каналів, такі як витік мови, конкретна інформація, що містить персональні дані, витік персональних даних, що обробляються в системах інформації через канал електромагнітного випромінювання та перешкод (ПЕМВП). Ці загрози, як правило, розглядаються стосовно інформаційних систем вищого класу, в яких обробляються спеціальні категорії персональних даних, що стосуються національної та расової приналежності людини, її релігійних чи філософських переконань, її здоров'я та її приватного життя. Відповідно до вимог законодавства розробляється спеціальна модель загроз для інформаційних систем, під час складання якої аналізуються окремі вразливості та загрози, розраховується їх актуальність, достатність існуючих та необхідність додаткових методів та засобів захист.

Надаючи свої персональні дані для зберігання, використання, модифікації тощо, суб’єкт очікує, що він буде захищений від несанкціонованого доступу, використання, розповсюдження та знищення. Для забезпечення безпеки оператори ПД повинні розробити систему протидії атакам зловмисників, і для цього потрібно спочатку визначити, від кого і яких дій слід боятися. Світова практика показує, що найбільш ефективними є СЗПД, створені на основі детальних загроз. Щоб визначити фактори, які можуть призвести до порушення безпеки, можна лише визначити загрози для персональних даних та їх джерел.

Будь-яка організація, ПП або фізична особа, чия діяльність пов'язана з обробкою приватних відомостей громадян, ризикує зіткнутися зі зловмисниками, які прагнуть їх отримати, змінити, знищити або передати третім особам без відповідного дозволу власника.

В рамках функціонування ІСПД загрози персональних даних - це всілякі умови і чинники, здатні за певних обставин викликати їх витік або неправомірне використання або вплив. Крім очевидних ситуацій, коли мова йде, наприклад, про промислове шпигунство, в дану категорію входять випадки неусвідомленого поширення інформації або передачі конфіденційних відомостей стороннім співробітниками підприємства. Завдання керівництва, а точніше, уповноважених осіб або залучених фахівців, полягає в пошуку «лазівок» в системі безпеки ПД і надалі вжиття заходів щодо їх усунення. Важливо розуміти, що виявлення ЗБПД не говорить про те, що крадіжка або втрата відомостей гарантовано станеться. Це свідчить про те, що є присутнім ймовірність виникнення небезпечних ситуацій, які слід запобігти.

Для кожного з існуючих видів інформаційних систем ПД потрібне створення особливої моделі факторів ризику. При цьому кількість обставин і дій, здатних тим чи іншим способом впливати на їх функціонування, дуже велике. Полегшити виявлення небезпек дозволяє їх поділ за такими ознаками:

За різновиди джерел. Виникають через властивостей використовуваних технічних засобів, стихійних явищ, дій персоналу або сторонніх осіб за допомогою міжнародних і внутрішніх російських мереж. Окрему групу становлять загрози ПД, спровоковані вірусами і апаратними закладками. Примітно, що не існує чітких інструкцій по виявленню недекларованих опцій, що змушує операторів діяти на свій страх і ризик. Найбільш безпечний варіант - користуватися ліцензованими програмами серійного випуску з численними позитивними відгуками від експертів.

По використовуваному способу реалізації. Оцінити фактори ризику можна через спеціальне вплив, витік технічними каналами, в результаті несанкціонованого доступу.

За типом ІСПД. В даному випадку прийнято виділяти не докладні списки, а класи в залежності від структури, яка наражається на небезпеку. Розрізняють УБ, що стосуються операцій в локальних ІС, на автоматизованих робочих місцях і в розподілених системах.

За здійснюваними несанкціонованими діями. Тут прийнято виділяти загрози, які при відсутності прямого впливу на зміст відомостей призводять до порушення конфіденційності ПД.

За уразливості. Ризики можуть бути обумовлені системним прикладним програмним забезпеченням, протоколами мережевого обміну, недостатньо ретельно опрацьованими технічними каналами засобами інформаційного захисту.

По тому, на який об'єкт здійснюється вплив - на автоматизоване робоче місце, мережі зв'язку, системний софт, прикладні утиліти, виділені кошти роботи з інформацією.

1.3. Джерела загроз системам захисту персональних даних.

Порушення режиму інформаційної безпеки може бути викликано як спланованими операціями зловмисників, так і недосвідченістю співробітників. Користувач повинен мати хоч якесь поняття про ІБ, шкідливий програмному забезпеченні, щоб своїми діями не завдати шкоди компанії і самому собі. Такі інциденти, як втрата або витік інформації, можуть також бути обумовлені цілеспрямованими діями співробітників компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали.

Основними джерелами загроз є окремі зловмисники («хакери»), кіберзлочинність групи і державні спецслужби, які застосовують весь арсенал доступних засобів, перерахованих і описаних вище. Щоб пробитися через захист і отримати доступ до потрібної інформації, вони використовують слабкі місця і помилки в роботі програмного забезпечення і веб-додатків, вади в конфігураціях

мережевих екранів і налаштуваннях прав доступу, вдаються до прослуховування каналів зв'язку і використання клавіатурних шпигунів.

Те, що буде проводитися атака, залежить від типу інформації, її розташування, способів доступу до неї і рівня захисту. Якщо атака буде розрахована на недосвідченість жертви, то можливо, наприклад, використання спам-розсилок.

Визначення каналів і причин, що призводять до несанкціонованого доступу і неправомірним діям, має першочергове значення, і з цього потрібно починати при побудові моделі ЗБПД. Всього є три типи джерел, кожен з яких має свої особливості.

Антропогенні

Особистість (суб'єктів може бути кілька), яка має можливість здійснювати операції з конфіденційною інформацією. Доступ може бути як санкціонованим, так і несанкціонованим. У цю групу входять наступні джерела загроз персональних даних:

Зовнішні - постачальники послуг, працівники контролюючих державних органів та аварійних служб, а також хакери, представники конкуруючих організацій. Їх дії можуть бути навмисними, тобто спрямованими на отримання відомостей, або неспеціальних, наприклад, якщо витік відбувається в результаті технічного збою або непрофесійного складання проекту інформаційної системи.

Внутрішні - штатні співробітники, зокрема, працівники програмного відділу, кадрової служби, техперсонал або представники служби безпеки компанії. В процесі своєї діяльності вони можуть піддавати СЗПД небезпеки через некомпетентність і помилкових дій, застосування неврахованого софта, спотворення і знищення компонентів програм, надання доступу уповноваженою особам або ігнорування правил зберігання ПД. Причиною витоку може стати також самовільна зміна параметрів системи захисту і замовчування фактів втрати інформації, що знаходиться в обмеженому доступі (паролів, ключів і т.п.).

Стихійні

Найбільш складно прогнозовані через величезного розмаїття, причин виникнення та способів прояву. Переважно це ті чинники, на які оператор ніяким чином не здатний вплинути:

- повені;
- цунамі;
- пожежі;
- урагани;
- зсуви;
- радіаційні катастрофи;
- військові конфлікти.

Техногенні

Ці джерела обумовлені застосовуваними технічними засобами і бувають двох різновидів:

внутрішні - це апаратні закладки, віруси та інші шкідливі програми, системи охорони та сигналізації, низькоякісний софт і обладнання, задіяне в процесі обробки персональних даних;

зовнішні - складові інфраструктурного призначення, наприклад, лінії телефонного та інтернет-зв'язку, системи опалення, каналізації, водопостачання, газопостачання.

Найбільш поширений спосіб нанести шкоди системі та викрадення даних – це комп’ютерний вірус. На даному етапі я б хотів більш детально про них розповісти, як працює кожен з вірусів та яку шкоду він може нанести.

Резидентні віруси.

Під терміном "резидентність" (DOS'овскій термін TSR - Terminate and Stay Resident) розуміється здатність вірусів залишати свої копії в системній пам'яті, перехоплювати деякі події (наприклад, звернення до файлів або дисків) і викликати при цьому процедури зараження виявлених об'єктів (файлів і секторів). Таким чином, резидентні віруси активні не тільки в момент роботи інфікованої програми, але і після того, як програма закінчила свою роботу. Резидентні копії таких вірусів залишаються життєздатними аж до чергового

перезавантаження, навіть якщо на диску знищені всі заражені файли. Часто від таких вірусів неможливо позбутися відновленням копій файлів з дистрибутивних дисків або backup-копій. Резидентна копія вірусу залишається активною і заражає новостворювані файли. Те ж вірно і для завантажувальних вірусів - форматування диска при наявності в пам'яті резидентного вірусу не завжди виліковує диск, оскільки багато резидентні віруси заражає диск повторно після того, як він відформатований.

Нерезидентні віруси.

Нерезидентні віруси, навпаки, активні досить нетривалий час - тільки в момент запуску зараженої програми. Для свого поширення вони шукають на диску незаражені файли і записуються в них. Після того, як код вірусу передає керування програмі-носію, вплив вірусу на роботу операційної системи зводиться до нуля аж до чергового запуску будь-якої зараженої програми. Тому файли, заражені нерезидентними вірусами значно простіше видалити з диска і при цьому не дозволити вірусу заразити їх повторно.

Стелс-віруси.

Стелс-віруси тими або іншими способами приховують факт своєї присутності в системі.

Використання Стелс-алгоритмів дозволяє вірусам чи цілком частково сховати себе в системі. Найбільш поширеним стелс-алгоритмом є перехоплення запитів ОС на читання / запис заражених об'єктів. Стелс-віруси при цьому або тимчасово лікують їх, або "підставляють" замість себе незаражені ділянки інформації. У разі макро-вірусів найбільш популярний спосіб - заборона викликів меню перегляду макросів. Відомі стелс-віруси всіх типів, за винятком Windows-вірусів - завантажувальні віруси, файлові DOS-віруси і навіть макро-віруси. Поява стелс-вірусів, що заражають файли Windows, є швидше за все справою часу.

Полиморфік-віруси.

Самошифрування і поліморфічність використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру виявлення

вірусу. Полиморфік-віруси (polymorphic) – це віруси, які досить важко виявити, що не мають сигнатур, тобто що не містять жодного постійної ділянки коду. У більшості випадків два зразки того самого поліморфік-вірусу не матимуть жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача.

До поліморфік-вірусів відносяться ті з них, детектування яких неможливо (або вкрай важко) здійснити за допомогою так званих вірусних масок - ділянок постійного коду, специфічних для конкретного вірусу. Досягається це двома основними способами - шифруванням основного коду вірусу з непостійним ключем і злучення набором команд розшифровщика або зміною самого виконуваного коду вірусу. Поліморфізм різного ступеня складності зустрічається у вірусах всіх типів - від завантажувальних і файлових DOS-вірусів до Windows-вірусів.

За середовищем «проживання» віруси можна розділити на:

- файлові;
- завантажувальні;
- макровіруси;
- мережеві.

Файлові віруси.

Файлові віруси або різними способами впроваджуються у виконувані файли (найбільш поширений тип вірусів), або створюють файли-двійники (компаньйон-віруси), або використовують особливості організації файлової системи (link-віруси).

Впровадження файлового вірусу можливо практично в усі виконувані файли всіх популярних ОС. На сьогоднішній день відомі віруси, що вражають всі типи виконуваних об'єктів стандартної DOS: командні файли (BAT), що завантажуються драйвери (SYS, в тому числі спеціальні файли IO.SYS і MSDOS.SYS) і виконувані двійкові файли (EXE, COM). Існують віруси, що вражають виконувані файли інших операційних систем - Windows 3.x,

Windows95 / NT, OS / 2, Macintosh, UNIX, включаючи VxD-драйвера Windows 3.x і Windows95.

Існують віруси, що заражають файли, які містять вихідні тексти програм, бібліотечні або об'єктні модулі. Можливий запис вірусу й у файли даних, але це трапляється або в результаті помилки вірусу, або при прояві його агресивних властивостей. Макро-віруси також записують свій код у файли даних - документи або електронні таблиці, - проте ці віруси настільки специфічні, що винесені в окрему групу.

Завантажувальні віруси.

Завантажувальні віруси заражають завантажувальний (boot) сектор флоппі-диска і boot-сектор або Master Boot Record (MBR) вінчестера. Принцип дії завантажувальних вірусів заснований на алгоритмах запуску операційної системи при включенні або перезавантаженні комп'ютера - після необхідних тестів встановленого обладнання (пам'яті, дисків і т.п.) програма системної завантаження зчитує перший фізичний сектор завантажувального диска (A :, C: або CD-ROM в залежності від параметрів, встановлених в BIOS Setup) і передає на нього управління.

У разі дискети або компакт-диска управління отримує boot-сектор, який аналізує таблицю параметрів диска (BPB - BIOS Parameter Block) вираховує адреси системних файлів операційної системи, зчитує їх в пам'ять і запускає на виконання. Системними файлами зазвичай є MSDOS.SYS і IO.SYS, або IBMDOS.COM і IBMBIO.COM, або інших в залежності від встановленої версії DOS, Windows або інших операційних систем. Якщо ж на завантажувальному диску відсутні файли операційної системи, програма, розташована в boot-секторі диска видає повідомлення про помилку і пропонує замінити завантажувальний диск.

У разі вінчестера управління отримує програма, розташована в MBR вінчестера. Ця програма аналізує таблицю розбиття диска (Disk Partition Table), обчислює адресу активного boot-сектора (зазвичай цим сектором є boot-сектор диска C :), завантажує його в пам'ять і передає на нього управління. Отримавши

управління, активний boot-сектор вінчестера проробляє ті ж дії, що і boot-сектор дискети.

При зараженні дисків завантажувальні віруси "підставляють" свій код замість якої-небудь програми, яка отримує управління при завантаженні системи. Принцип зараження, таким чином, однаковий у всіх описаних вище способах: вірус "змушує" систему при її перезапуску вважати в пам'ять і віддати управління не оригінальному коду завантажувача, але коду вірусу.

Зараження дискет проводиться єдиним відомим способом - вірус записує свій код замість оригінального коду boot-сектора дискети. Вінчестер заражається трьома можливими способами - вірус записується або замість коду MBR, або замість коду boot-сектора завантажувального диска (зазвичай диска C :), або модифікує адресу активного boot-сектора в Disk Partition Table, розташованої в MBR вінчестера.

Макро-віруси.

Макро-віруси заражають файли-документи й електронні таблиці декількох популярних редакторів. Макро-віруси (macro viruses) є програмами на мовах (макро-мовах), вбудованих в деякі системи обробки даних (текстові редактори, електронні таблиці і т.п.). Для свого розмноження такі віруси використовують можливості макро-мов і за їх допомогою переносять себе з одного зараженого файлу (документа або таблиці) в інші. Найбільшого поширення набули макро-віруси для Microsoft Word, Excel і Office97. Існують також макро-віруси, що заражають документи Ami Pro і бази даних Microsoft Access.

Мережеві віруси.

До мережевих відносяться віруси, які для свого поширення активно використовують протоколи і можливості локальних і глобальних мереж. Основним принципом роботи мережного вірусу є можливість самостійно передати свій код на віддалений сервер або робочу станцію. "Повноцінні" мережні віруси при цьому володіють ще і можливістю запустити на виконання свій код на віддаленому комп'ютері або, принаймні, "підштовхнути" користувача

до запуску зараженого файлу. Приклад мережевих вірусів - так звані IRC-черв'яки.

IRC (Internet Relay Chat) - це спеціальний протокол, розроблений для комунікації користувачів Інтернет в реальному часі. Цей протокол надає їм можливість Інтернет - "розмови" за допомогою спеціально розробленого програмного забезпечення. Крім відвідування загальних конференцій користувачі IRC мають можливість спілкуватися один-на-один з будь-яким іншим користувачем. Крім цього існує досить велика кількість IRC-команд, за допомогою яких користувач може отримати інформацію про інших користувачів і каналах, змінювати деякі установки IRC-клієнта та інше. Існує також можливість передавати і приймати файли - саме на цій можливості і базуються IRC-черв'яки. Як виявилося, потужна і розгалужена система команд IRC-клієнтів дозволяє на основі їх скриптів створювати комп'ютерні віруси, передають свій код на комп'ютери користувачів мереж IRC, так звані "IRC-черв'яки". Принцип дії таких IRC-хробаків приблизно однаковий. За допомогою IRC-команд файл сценарію роботи (скрипт) автоматично надсилається з зараженого комп'ютера кожному знову приєднався до каналу користувачеві. Присланий файл-сценарій заміщає стандартний і при наступному сеансі роботи вже знову заражений клієнт буде розсилати хробака. Деякі IRC-черв'яки також містять троянський компонент: по заданим ключовим словами виробляють руйнівні дії на уражених комп'ютерах. Наприклад, хробак "pIRCH.Events" по певній команді стирає всі файли на диску користувача.

Існує велика кількість сполучень - наприклад, файлово-завантажувальні віруси, що заражають як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи, часто застосовують оригінальні методи проникнення в систему, використовують стелс і поліморфік-технології. Інший приклад такого сполучення - мережний макро-вірус, який не тільки заражає редаговані документи, але і розсилає свої копії по електронній пошті.

1.4. Висновки до першого розділу.

Підсумовуючи усе те, про що йшла мова у першому розділі, можна зробити висновок, що персональні дані людини «приваблюють» дуже велику кількість зловмисників. Адже через них можна нанести дуже велику шкоду тій чи іншій особі. Саме тому захист персональних даних так чи інакше є дуже важливим. Але цей захист потрібно весь час оновлювати, тому що злодії знаходять все нові та нові методи атак. З часом в системі, в якій зберігаються ПД, з'являється все більше інформації, тому злодіям все легше до неї дістатися. І це не кажучи про те, що є і інші фактори, які впливають на захист.

Саме тому я поставив задачу створення та опису надійного захисту на основі вже існуючих систем. Аналіз загроз показує, що небезпека може існувати у всьому, починаючи здій конкретної люди і закінчуючи природою. Саме тому було прийнято рішення зібрати всі найкращі якості існуючих систем і об'єднати в одну.

Завдяки цій роботі, яка більш детально буде описана у другому та третьому розділах. Буде усунуто деякі недоліки та запропоновані нові рішення проблеми захисту даних. Мною буде розглянуто засоби захисту, програмне та апаратне забезпечення, яке буде перешкоджати неправомірним діям зловмисників.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМ ЗАХИСТУ ДАНИХ

2.1. Підходи аудиту, організації та забезпечення захисту персональних даних.

Аудит існуючої системи захисту персональних даних - це дослідження різних процесів обробки персональних даних. Також це аналіз документації, пов'язаної з організаційно-розпорядчим напрямком діяльності компанії, всілякі рекомендації, доробка вже наявної системи і багато іншого.

Аудит захисту персональних даних також може включати в себе супровід наявної системи при наявності змін в законодавстві або при появі будь-яких загроз. Додатково це можуть бути технічні заходи щодо створення системи захисту персональних даних.

Аудит персональних даних триває експертно-документальним аналізом. Для цього використовується технічна, організаційно-розпорядча документація. Обов'язково проводиться опис технічних рішень, різних функціональних схем, виконується перевірка документів на відповідність вимогам законодавства.

Важливо розуміти, для чого потрібно вживати заходів щодо захисту персональних даних. Якщо перевіряється документація, навіть частина інформаційної системи персональних даних не відповідають вимогам законодавства, то це послужить причиною того, що виникне відповідальність за порушення вимог щодо захисту персональних даних.

Проблема регулювання процесу збору персональних даних, підтримка інформаційної безпеки та інші супутні питання, пов’язані з роботою з персональними даними, у нашій країні на сьогодні відносно вирішені та відомі широкому колу юристів. Очевидно, законодавство не є досконалим і потребує вдосконалення, але основні положення регулюються Законом України "Про захист персональних даних" від 1 червня 2010 р. № 2297-VI. Отже, відповідно до ст. 12 зазначеного Закону, збір персональних даних є частиною процесу їх обробки, який передбачає дії з відбору або впорядкування інформації про особу.

Суб’єкт персональних даних повідомляється про власника персональних даних, склад та зміст зібраних персональних даних, його права, визначені Законом, мету збору персональних даних та осіб, яким передаються його персональні дані: під час збору персональних даних, якщо вони збираються у суб’єкта персональних даних, а в інших випадках - протягом тридцяти робочих днів з дати збору персональних даних. Окрім вищезазначеного Закону, юридичні та фізичні особи мають можливість вирішувати питання, пов’язані з власною інформаційною безпекою, використовуючи положення Цивільного кодексу України, Закону України «Про інформацію» та інших актів українського законодавства [16].

Менш дослідженим та більш цікавим питанням з точки зору кроків у майбутні та європейські інтеграційні амбіції України є ознайомлення, вивчення та аналіз регулювання захисту персональних даних, зокрема, їх збору у країнах Європейського Союзу. Найактуальнішою та найбільш активно розвиненою зараз є проблема захисту персональних даних та інформаційної безпеки в Інтернеті. Отже, 25 травня 2018 року для користувачів, які перебувають у Європейській економічній зоні (ЄЕЗ), набрали чинності Правила нового Закону про захист персональних даних в Інтернеті. Тут слід розуміти, що ЄЕЗ охоплює не лише країни власне Європейського Союзу, а й країни Європейської асоціації вільної торгівлі (ЄАВТ), крім Швейцарії.

Угода про створення Європейської економічної зони була підписана в 1992 році і набула чинності 1 січня 1994 року. ЄЕЗ базується на тих самих "чотирьох свободах", що і Європейське Співтовариство: вільне переміщення товарів, людей, послуг та капітал між країнами ЄЕЗ. Таким чином, країни ЄАВТ, які є членами ЄЕЗ, мають режим вільної торгівлі з Європейським Союзом. Це дозволяє таким країнам ЄАВТ, як Ісландія, Норвегія та Ліхтенштейн, брати участь у єдиному європейському ринку без вступу до ЄС. Відповідно до Угоди про Європейський економічний простір, розширення ЄС тягне за собою розширення Європейського економічного простору. Тому зараз Європейський економічний простір охоплює 30 країн [16].

Нові правила, наведені вище, позначаються абревіатурою GDPR (Загальний регламент про захист даних) і застосовуються до всіх учасників світового Інтернету, які беруть участь у зборі, зберіганні або обробці персональних даних. Хоча Закон прийнято для захисту європейських даних, глобальний характер Інтернету означає, що GDPR встановлює стандарт конфіденційності даних у всьому світі. Майже всі великі інтернет-компанії, включаючи Google, Facebook та Twitter, підпадають під дію GDPR.

У цілях GDPR - забезпечити ще більший захист персональних даних людини, включаючи, але не обмежуючись, її релігійні чи політичні переконання. Штрафи за недотримання правил є значними: до 20 мільйонів євро або 4% від загального обороту за порушення. Крім того, GDPR надає користувачам можливість компенсувати будь-яке суттєве та / або нематеріальне порушення GDPR.

GDPR застосовується до даних, які збираються, обробляються та / або зберігаються в Європі, незалежно від того, де дані збираються. Якщо, наприклад, фізична особа має в Україні інтернет-магазин з інформаційним бюлетенем і на нього підписався принаймні один потенційний клієнт з Європейського Союзу, то такий інтернет-магазин підпорядковується правилам GDPR, що відкриває нові можливості для юристів покращити свої знання та надати допомогу клієнтам.

Важливою умовою GDPR є те, що з моменту набрання чинності цим Законом забороняється передавати дані за межі Європейського Союзу в будь-яку країну, яка ЄС не вважає дотриманням вимог законодавства про захист персональних даних. Якщо дані передаються особисто за межі ЄС для обробки або зберігання, то слід отримати явну згоду від користувача, який володіє даними [16].

У будь-якій ситуації, коли ви запитуєте дані користувача, спочатку запитайте себе: як це вплине на права власника цих даних? GDPR визначає такі юридичні права, які мають власники даних: право доступу, право на об’єкт, право на інформування, право на виправлення, право на перенесення даних,

право на видалення даних, право не підлягати автоматичному прийняттю рішень, право обмежувати обробку даних [16].

Однак власники даних також мають права. Наприклад, якщо користувач підписався на ваш бюлетень. З часом він вирішує, що більше не хоче отримувати розсилку та відписується. У цьому випадку вам просто потрібно назавжди стерти електронну адресу цього користувача. Однак, коли користувач підписується на розсилку, ви повинні знати його IP-адресу, щоб відповідати його згоді на отримання розсилки (як і потрібно), оскільки ви маєте право зберігати ці дані, щоб підтвердити, що ваш веб-сайт відповідає правила GDPR.

Важливо розуміти, що регулятор Європейського Союзу не зобов'язаний доводити вашу невідповідність правилам. Ваша юридична відповідальність - довести, що ви відповідаєте вимогам, а невиконання цього - саме по собі не відповідає вимогам. Також слід вийти за межі принципу конфіденційності за замовчуванням: користувачеві не потрібно вживати жодних дій для забезпечення конфіденційності. Якщо користувач нічого не робить, його дані розглядаються як приватні. Вбудовування конфіденційності в проект: Конфіденційність не додається до проекту із зворотною силою, це невід'ємний компонент будь-якого продукту чи системи. Також потрібно буде провести оцінку впливу на конфіденційність, а потреба у співробітнику з питань захисту даних також буде обов'язковою умовою для великих компаній. Крім того, слід зазначити, що відповідно до GDPR, згода чітко визначена для забезпечення захисту прав користувачів: вона повинна бути чіткою, перевіряється та надаватися добросовісно. Згода на цифрові послуги від дитини до 16 років також вимагає згоди батьків.

Слід розуміти, що якщо будь-яка з цих вимог не відповідає згоді, яку ви отримали від ваших користувачів, тоді буде вважатися, що ви не маєте згоди, незалежно від намірів ваших користувачів. Також GDPR, зокрема, вимагає спеціальної декларації про конфіденційність [16].

Під захистом персональних даних мається на увазі комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки і

конфіденційності персональних даних, які обробляються як в ІСПД, так і поза ІСПД.

Оператор до початку обробки персональних даних зобов'язаний повідомити уповноважений орган із захисту прав суб'єктів персональних даних про свій намір здійснювати обробку персональних даних, за винятком таких випадків:

1) відносяться до суб'єктів персональних даних, яких пов'язують з оператором трудові відносини;

2) отриманих оператором у зв'язку з укладенням договору, стороною якого є суб'єкт персональних даних, якщо персональні дані не поширюються, а також не надаються третім особам без згоди суб'єкта персональних даних і використовуються оператором виключно для виконання зазначеного договору та укладення договорів з суб'єктом персональних даних;

3) що відносяться до членів (учасників) громадського об'єднання чи релігійної організації та оброблюваних відповідними громадським об'єднанням або релігійною організацією, для досягнення законних цілей, передбачених їх установчими документами, за умови, що персональні дані не будуть поширюватися без згоди в письмовій формі суб'єктів персональних даних;

4) є загальнодоступними персональними даними;

5) включають в себе тільки прізвища, імена та по батькові суб'єктів персональних даних;

6) необхідних з метою одноразового пропуску суб'єкта персональних даних на територію, на якій знаходиться оператор, або в інших аналогічних цілях;

На етапі обстеження інформаційних систем ПД виконуються наступні роботи:

- формується перелік ПД, інформаційних систем і технічних засобів, що використовуються для їх обробки;
- визначаються підрозділи і працівники, які оброблятимуть ПД;
- визначаються категорії ПД;

- розробляється опис об'єкта захисту, включаючи склад і характеристики засобів обробки даних;
- проводиться попередня класифікація інформаційних систем ПД (перегляд класу проводиться на розсуд оператора в будь-який час);
- здійснюється оцінка необхідних заходів і витрат по приведенню інформаційних систем ПД у відповідність з вимогами.

Результатами робіт на етапі обстеження є:

- перелік ПД і категорії ПД;
- переліки інформаційних систем і технічних засобів, що використовуються для обробки ПД, і аналіз їх стану;
- склад наявних заходів і засобів захисту ПД;
- перелік підрозділів і співробітників, що обробляють ПД;
- класифікація інформаційних систем, що обробляють ПД на типові спеціальні;
- акти класифікації інформаційних систем, що обробляють ПД;
- опис об'єктів захисту;
- уточнення типові моделі загроз і вимоги до систем захисту ПД;
- перелік необхідних заходів і орієнтовна вартість робіт по приведенню інформаційних систем ПД у відповідність з вимогами.

Слід оцінити можливість знеособлення або зниження класів інформаційних систем і провести необхідні роботи повторно.

2.2. Засоби забезпечення захисту персональних даних.

Компанії повинні встановити технічні та організаційні заходи безпеки для забезпечення конфіденційності та цілісності персональних даних з метою збереження безпеки даних від модифікації, втрати, передачі та несанкціонованого доступу. Усі заходи щодо захисту даних повинні застосовуватися з найвищим ступенем захисту персональних даних. Заходи

безпеки повинні бути частиною системи захисту даних. Далі я розгляну деякі з них та розповім про них більш детально.

Фізична безпека.

Безпека об'єкта фізична - стан захищеності життєво-важливих інтересів (об'єкта) від погроз, джерелами яких є злочинні протиправні (несанкціоновані) дії фізичних осіб (порушників). Сюди входить захист об'єктів, обладнання для запобігання випадкам випадкових випадків або форс-мажорних обставин.

Концепція безпеки - загальний задум забезпечення безпеки об'єкта від прогнозованих загроз.

Уразливість (об'єкта) - ступінь невідповідності вжитих заходів захисту (об'єкта) прогнозованим загрозам або заданим вимогам безпеки.

Надзвичайна ситуація (на об'єкті) - стан, при якому (на об'єкті) порушуються нормальні умови життя і діяльності людей, виникає загроза їх життю і здоров'ю, завдається шкода майну та навколишньому природному середовищу.

Ефективність системи фізичної безпеки - ймовірність виконання системою своєї основної цільової функції по забезпеченню захисту об'єкта від загроз, джерелами яких є злочинні протиправні (несанкціоновані) дії фізичних осіб (порушників).

«Система фізичного захисту» являє собою сукупність правових норм, організаційних заходів і інженерно-технічних рішень, спрямованих на захист життєво-важливих інтересів і ресурсів підприємства (об'єкта) від погроз, джерелами яких є злочинні (несанкціоновані) фізичні впливу фізичних осіб - порушників (терористів, злочинців, екстремістів і ін.).

Сучасні СФЗ будуються на базі широкого застосування інженерно-технічних і програмних засобів і містять такі основні складові частини (підсистеми):

- система контролю і управління доступом персоналу (СКУД);
- система охоронної сигналізації (СОС);
- система телевізійного спостереження (СТН);

- система оперативного зв'язку та оповіщення;
- забезпечують системи (освітлення, електроживлення, охоронного освітлення та ін.).

При створенні сучасних СФЗ, як правило, ставиться також і завдання захисту життєво важливих центрів і систем об'єкта від ненавмисних, помилкових або некомпетентних дій персоналу, які за характером можливого збитку наближаються до НСД зовнішніх порушників.

З огляду на складність вирішуваних завдань, створення СФЗ важливих об'єктів не може базуватися на досить часто застосовується на практиці принципі «розумної достатності», а вимагає комплексного наукового підходу. Такий підхід має на увазі проектування СФЗ важливих об'єктів в дві стадії:

- концептуальне (системне) проектування;
- робоче проектування.

Основними етапами стадії концептуального проекту є:

1) Аналіз вразливості об'єкта та існуючої СФЗ;

2) Розробка принципів фізичного захисту об'єкта;

3) Розробка техніко-економічного обґрунтування створення СФЗ.

Логічна безпека.

Сюди входять заходи щодо ідентифікації та автентифікації людей або користувачів, уповноважених на доступ та зміну персональних даних.

Логічна безпеку відноситься до процесу використання програмних методів для аутентифікації привілеїв користувача в конкретній комп'ютерній мережі або системі. Ця концепція є частиною більш повної області комп'ютерної безпеки, яка включає в себе як апаратні, так і програмні методи для захисту терміналу або мережі. Під час обговорення логічної безпеки слід враховувати різні використовувані методи, які включають імена користувачів і паролі, безпеку токенів і двосторонню аутентифікацію в системі.

Аутентифікація по паролю, мабуть, найпоширеніший і знайомий тип логічної захисту. Той, хто коли-небудь використав сайт онлайн-банкінгу або навіть систему соціальних мереж, буде знайомий з цією концепцією. Коли в

мережі налаштоване використання аутентифікації по паролю, користувачі, які намагаються увійти в конкретний термінал в мережі, спочатку повинні підтвердити свої облікові дані, ввівши ім'я користувача та пароль. Основною перевагою тут є простота; користувачам не потрібно нічого, крім імені користувача, яке було запам’товано, та пароля, щоб отримати доступ до системи. Одним з основних недоліків є те, що у комп'ютера немає можливості перевірити, чи є користувач, який використовує певну комбінацію імені користувача та пароля, авторизованим користувачем; тому недобросовісні користувачі можуть вкрасти імена користувачів і паролі, щоб зламати систему.

Безпека токенів - це логічна техніка безпеки, яка включає використання карток ключів або інших фізичних пристроїв для аутентифікації користувача в мережі. Після того, як користувач проводить свою картку в системі, йому надається доступ до комп'ютера. Деякі популярні типи токен-пристроїв містять постійно мінливий код, який кожну хвилину або близько того перемикається на нове значення, забезпечуючи захист системи від осіб, які намагаються дублювати захисні карти. Знову ж, як і при аутентифікації по паролю, немає реального захисту від осіб, що викрадають чужу карту доступу для отримання доступу до системи.

Двостороння аутентифікація передбачає обмін питаннями і відповідями між користувачем і комп'ютерною системою. Коли користувач намагається увійти в систему, комп'ютер відправить питання, відомий як «виклик», і кінцевий користувач повинен відповісти з правильним результатом, щоб отримати доступ до системи. Перевага цього типу логічної техніки безпеки полягає в тому, що система не прив'язана до певної комбінації імені користувача і пароля; може бути будь-яка кількість проблем, що не дозволяють неавторизованих користувачам легко отримати доступ до системи, просто вкрадено одну конкретну комбінацію імені користувача та пароля.

Програми.

Це одна з основних областей курсу захисту даних. Він представляє дозволи, якими повинна керувати система обробки персональних даних, щоб

забезпечити належне використання даних, запобігаючи участі несанкціонованих користувачів, відокремлення середовищ та контроль контролю проникнення.

Програмна захист інформації - система спеціальних програм, що включаються до складу програмного забезпечення, що реалізують функції захисту інформації. Захисний програмний код може виступати як окремо, в якості окремого захисного програмного продукту, так і включатися до складу інших, багатофункціональних програм, з метою захисту оброблюваних ними даних або самозахисту від шкідливого коду. Так як захисні функції багатофункціональних програм часто навіть не мають істотних засобів самозахисту і за визначенням програють спеціалізованому захисному програмному забезпеченню, будь-яка значуща комп'ютерна система вимагає розгортання та повноцінної інтеграції програмних засобів захисту інформації на всіх або хоча б найбільш уразливих елементах системи.

- Програмні засоби захисту інформації діляться на типи так:
- Контроль доступу
- Анти-кейлоггери
- Анти-шпигуни (anti-spyware)
- Анти-експлуататори (anti-subversion)
- Анти-модифікатори (anti-tampering)
- антивіруси
- шифрування
- Брандмауери (firewall)
- Системи виявлення вторгнень
- Системи запобігання вторгнень
- Пісочниця

Не слід плутати програмну захист інформації з захистом комп'ютерів від несанкціонованого використання або захистом мережі комп'ютерів, не дивлячись на те, що їх функції багато в чому перетинаються. При використанні даного підходу захищається сама інформація, будь то операційна система, спеціалізоване програмне забезпечення або якийсь документ в цифровому

вигляді. При цьому такий захист підрозділяється на захист даних і захист програм.

Повноцінна програмна захист інформації на сервері або робочому комп'ютері вимагає використання різних типів захисних програм або спеціалізованих захисних рішень, які суміщають в собі декілька типів захисту одночасно.

Наприклад, важливо розуміти, що панівний на даний момент антивірусний підхід, зазвичай об'єднує в собі антивіруси, анти-шпигуни, анти-експлуататори і анти-модифікатори, недостатній проти цільових атак, так як він заснований на порівнянні програмного коду з наявними у виробника сигнатурами шкідливого коду. Наявна в деяких випадках можливість застосування поведінкового аналізу також не дає гарантії збереження даних і збереження працездатності системи. Аналогічно, контроль доступу сам по собі не здатний гарантувати використання програм і даних виключно мають право на це особами, так як крім програмних вразливостей такий тип захисту може бути «розкритий» звичайної соціальною інженерією без використання високотехнологічних способів нападу в принципі. Системи виявлення вторгнень можуть допомогти при подальшому розслідуванні інциденту, але без систем запобігання вторгнень пошкодження, отримані при атаці, можуть виявитися дуже серйозними, щоб розслідування в принципі знадобилося. Шифрування даних може допомогти проти спроб вкрасти ці дані, але не зупинить зловмисника, який бажає ці дані знищити.

Подібні недоліки вузькоспеціалізованої захисту можна знайти в будь-якій комбінації малої кількості схожих типів програмних засобів захисту інформації, тому захист завжди повинна бути заснована на безлічі паралельних і часто перетинаються алгоритмах. При використанні декількох рішень це загрожує внутрішніми конфліктами в системі, тому найбільш логічним висновком є використання комплексних захисних систем, що використовують більшість згаданих типів захисту інформації для захисту даних, захисту програм і самозахисту від вторгнень, копіювання, модифікації і знищення.

Всі захисні програмні рішення SafenSoft мають модульну структуру і єдиним керуючим сервером, що гарантує можливість повноцінної інтеграції в саму комплексну IT-інфраструктуру організації, при цьому захищаючи саме ті області системи, які захищені найслабше. Сумісність з вже встановленими захисними рішеннями сторонніх виробників дозволяє виключити стандартну дилему побудови захищеної інфраструктури про вибір того чи іншого виробництва рішень, що гарантує саму об'єктивну оцінку ефективності наших продуктів від клієнтів, які скористалися нашими послугами по забезпеченню інформаційної безпеки в їхніх організаціях.

Шифрування.

Це включає впровадження та використання алгоритмів шифрування, ключів, паролів та конкретних заходів захисту для забезпечення цілісності та конфіденційності конфіденційних персональних даних у системі захисту даних.

Шифрування даних - процес давно відомий і досить зрозумілий. Дві сторони використовують спеціальні ключі шифрування і дешифрування. Навіть якщо в процесі передачі інформації від відправника до одержувача дані будуть перехоплені зловмисником, прочитати їх без ключів шифрування неможливо. Таким чином, перехоплення зашифрованої інформації стає безглуздим. Як ви розумієте, не дивлячись на те, що шифрування даних, як ідея, - це просто, реальне втілення задуму в життя пов'язане зі значними труднощами. У шифрування, як у медалі, є дві сторони. Постійно використовувати надскладне шифрування даних, яке неможливо зламати, недоцільно, тому що це створює великі труднощі одержувачу. У разі, якщо шифрування даних проводиться з використанням занадто простих ключів шифрування, теж не дуже добре: зусиль багато, сенсу – нуль. В такому випадку вже простіше обійтися взагалі без шифрування. Всі розуміють, що будь-яка хороша система повинна бути збалансована. Шифрування даних - не виняток: інформація і дані повинні відправлятися швидко, але, при цьому, дані повинні залишатися в безпеці. В даний час, віртуальна приватна мережа - VPN, яка застосовує шифрування даних, є хорошим прикладом швидкого і безпечного інтернет з'єднання. VPN в

основному займається виявленні слабких місць в системі безпеки інтернет користувачів та маскування IP адреси для великої кількості людей. Преміум-провайдери VPN приділяють максимум своєї уваги комплексного забезпечення безпеки користувачів, а не тільки тому, щоб з'єднання не було зламано. На щастя, висококласні професіонали, які використовують шифрування даних для захисту вашої інформації, зазвичай мають так багато можливостей, що будь-якому зловмисникові буде набагато простіше відмовитися від свого задуму, ніж слідувати їй.

Якщо сказати просто, то шифрування даних - це видозміна інформації для того, щоб вона стала нерозпізнаваною для сторонніх. Зазвичай, шифрування даних відбувається за допомогою будь-якого методу шифрування або ключа (пароля) шифрування / дешифрування, який відомий лише двом сторонам: відправнику і одержувачу. Цифрове шифрування даних складніше, ніж шифрування рукописне, але воно засноване на тих же принципах.

Розрізняють два типи шифрування, кожен з яких використовує різні методи шифрування і дешифрування інформації. Найбільш поширеним типом є симетричне шифрування даних, яке передбачає, що відправник і передбачуваний одержувач використовують один і той же ключ для шифрування і дешифрування повідомлення. Інший, більш складний тип шифрування даних називається асиметричним, в цьому випадку відправник і одержувач використовують різні ключі для шифрування і розшифровки повідомлення.

Шифрування даних перетворює передану інформацію в купу непов’язаних символів, які неможливі для читання і розуміння випадковому, сторонній людині. Тільки людина, що має ключ дешифрування зможе розпізнати цю інформацію. Оскільки більшість даних, включаючи носії, відображаються у вигляді тексту, вони можуть бути зашифровані таким же чином. Шифрування даних забезпечує конфіденційність будь-яких типів даних.

Нарешті, необхідно зрозуміти одну річ - шифрування даних досить складна інтелектуальна задача. У фільмах нам часто показують пролазливих секретних агентів, які читають закодовані повідомлення з келихом мартіні в одній руці і

пістолетом в інший. Насправді люди, які виконують шифрування даних, рідко бувають влучними стрілками, але досить часто вони є талановитими математиками, здатними придумувати коди, алгоритми і ключі шифрування для того, щоб забезпечити кожному користувачеві надійне шифрування, здатне протистояти будь-якій атаці. Звичайний користувач отримує вже готовий продукт у вигляді спеціальних додатків.

Мережевий зв'язок.

Мережева модель даних - логічна модель даних, що є розширенням ієрархічного підходу, сувора математична теорія, що описує структурний аспект, аспект цілісності і аспект обробки даних в мережевих базах даних. Під мережевим зв'язком мається на увазі використання корпоративних служб захисту даних, що включає використання системи моніторингу мережі, яка постійно контролює мережевий зв'язок та блокує будь-які підозрілі дії або порушення безпеки.

Ці аспекти навчальної програми із захисту даних становлять мінімальні вимоги, тому компанії та / або організації повинні вжити додаткових неминучих заходів для забезпечення більшого захисту. Компанії повинні скористатися допомогою консультантів служби захисту даних для впровадження системи захисту персональних даних.

2.3. Висновки до другого розділу.

У другому розділі мною було підходи до аналізу персональних даних, їх організацію. Також було представлено методи та засоби захисту, починаючи від програмного і закінчуючи фізичним. В наш час, в еру комп'ютерних технологій, дуже складно захистити дані. Тому підприємствам, в моєму випадку, дуже важливо гарантувати своїм працівникам їх безпеку. Адже жоден не хоче, щоб у вільному доступі з'явилась їх особиста інформація. Це також негативно впливає на компанію, підриваючи до неї довіру.

Мною вже були розглянуті закони, які контролюють та забезпечують конфіденційність персональних даних. Також я представив підготовчий етап створення системи безпеки, у якій йдеться про попередній розгляд та класифікацію персональних даних, можливі загрози.

У цьому розділі я розглянув вже деякі засоби захисту. У наступній частині я маю на меті більш детально розглянути засоби апаратного та програмного захисту, переглянути вже існуючі системи захисту та розробити нову, яка буде більш детально захищати персональну інформацію.

РОЗДІЛ 3. СИСТЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПІДПРИЄМСТВІ

3.1 Дослідження апаратного забезпечення системи захисту.

Апаратні засоби захисту інформаційних систем - засоби захисту інформації та інформаційних систем, реалізованих на апаратному рівні. Дані засоби є необхідною частиною безпеки інформаційної системи, хоча розробники апаратури зазвичай залишають вирішення проблеми інформаційної безпеки програмістам.

Завдання апаратного захисту обчислень була вирішена радянськими розробниками створенням обчислювального комплексу Ельбрус 1. В основі лежить ідея контролю типів на всіх рівнях системи, в тому числі і на апаратному. І основна заслуга розробників в планомірної її реалізації.

Розробниками Ельбрусу була запропонована наступна модель захищеної інформаційної системи.

Інформаційну систему в загальному випадку можна уявити, як інформаційний простір і обслуговуюче його обробляє пристрій. Обчислення розбиваються на окремі обчислювальні модулі, розташовані в інформаційному просторі. Схему реалізації обчислень можна представити таким чином: обробляє пристрій під керівництвом програми може звертатися до цього простору, читаючи і редагуючи його.

Для опису системи введемо поняття:

- вузол;
- посилання;
- контекст програми.

Вузол - осередок даних довільного обсягу разом із посиланням на неї з обробного пристрою.

Посилання не тільки описує дані, а й містить всі права доступу до них. Система повинна забезпечувати контроль над тим, щоб в операціях, які використовують посилання, не були використані дані інших типів а в операціях з аргументами інших типів посилання не могла бути модифікована.

Контекст програми - безліч всіх даних доступних для обчислень в конкретному модулі.

Захист на рівні розширень Bios.

Захист ресурсів ПЕОМ на апаратному рівні може бути реалізована з використанням механізмів розширень Bios. У ПЕОМ, реалізованих на платформі Intel, первинна активізація обчислювальних ресурсів комп'ютера проводиться кодом процесора, що зберігається в основному Bios. При включенні харчування код основного Bios «проектується» в область пам'яті F000 і управління передається на точку входу, певну виробником Bios. Після цього код Bios виробляє тестування обладнання, ініціалізацію векторів переривань, активізацію відеосистеми і деякі інші дії, що залежать від специфіки Bios. До складу коду Bios входить типова процедура пошуку так званих розширень Bios (Bios Extention). Розширення Bios - фрагмент виконуваного коду, оформлений за правилами, наведеними нижче, на який (у разі дотримання цих правил) передається управління в ході процедури пошуку розширень. Пошук розширень полягає в скануванні з кроком 512 байт області пам'яті з C000 до F000 з метою знаходження двобайтового сигнатури 55AA. Після знаходження цієї сигнатури аналізується наступний (третій, починаючи з 55) байт, який вказує область розширення Bios в 512-байтних сторінках (або блоках).

Якщо у зазначеній позиції знаходиться число, відмінне від 0, то обчислюється арифметична байтова контрольна сума від області пам'яті з байту 55 на довжину, зазначену в третьому байті. У разі збігу цієї суми з 0 на четвертий (від першого байту 55) байт передається керування.

Якщо в тілі коду, на який передано управління, виявиться процедура RETF (з урахуванням стану стека на момент виклику розширення), то відбудеться

повернення до основного Bios (тобто до процедури подальшого пошуку розширень).

Таким чином, є механізм для реалізації ряду захисних функцій на апаратному рівні ПЕОМ, тобто на рівні, що «хронологічно» знаходиться на рівні завантаження операційної системи. З урахуванням того, що обсяг розширення Bios не може бути дуже великим, на цьому рівні може бути реалізований досить невеликий обсяг значущих для безпеки КС функцій, а саме:

- ідентифікація та аутентифікація користувача (можливо, з використанням специфічного апаратного носія;
- заборона несанкціонованої завантаження ОС з обраних носіїв (наприклад з CD-ROM);
- контроль незмінності або цілісності апаратної або програмної компоненти ПЕОМ.

Треба зауважити, що перший розширений Bios, код якого буде виконаний, - це розширення, що проектується відкритий (VideoBios). Воно розташоване за адресою C000. Використовуючи програми отримання дампа пам'яті, можна переконатися в наявності зазначених вище заголовків і команд.

Програмування користувачем розширеного Bios пов'язано з вирішенням ряду технічних проблем. Перша з них пов'язана з тим, що програмування в даному випадку доцільно на мові низького рівня. Друга пов'язана з тим, що зміна станів змінних програми при її незмінному розміщенні в ПЗП неможливо. Це зумовлює необхідність коректного переміщення коду в ОЗП з передачею керування. Далі варто згадати про те, що на етапі виконання коду Bios доступний тільки ряд сервісних функцій, які можуть бути використані для програмування на низькому рівні, - це сервіс клавіатури, реалізований в обробниках 9h і 16h переривань, відеосервіс 10h переривання і сервіси диска 13h переривання.

Крім того, коректне завершення фрагментів коду розширень являє собою окрему задачу. Як зазначалося вище, повернення до виконання основного Bios відбувається по команді RETF. Однак якщо реалізований користувачем код

розширення містить аварійні виходи (наприклад, в разі невірної аутентифікації користувача), то коректне переривання виконання може бути виконано через апаратне перезавантаження комп'ютера.

Нарешті, про те, яким чином можна реалізувати розширення Bios. В даний час існує значна кількість мережевих карт з місцем розміщення ПЗУ або флеш, а також значне число засобів захисту (наприклад, плати АКОРД), які дають можливість перепрограмування коду розширень Bios, в якому можна закласти необхідний механізм пральний ідентифікації і аутентифікації користувачів (наприклад, триразовий запит пароля).

Захист на рівні завантажувач операційного середовища.

Локалізація захисних механізмів в структурах, пов'язаних з організацією початкового завантаження операційних систем, дозволяє вирішити ряд важливих завдань комп'ютерної безпеки. Це завдання, пов'язані з «ранньої» ідентифікацією й аутентифікації користувачів (за відсутності апаратних засобів захисту), захистом від несанкціонованої завантаження операційної системи, а також отриманням спеціального виду завантажувальних носіїв.

Розглянемо дані проблеми докладніше. Перша проблема виникає в тому випадку, коли процедури ідентифікації і аутентифікації не вдається реалізувати на етапі ініціалізації апаратної компоненти комп'ютера (зокрема, неможливо реалізувати зазначені процедури в розширенні Bios). При розміщенні процедур ідентифікації-аутентифікації спільно з процедурами початкового завантаження вдається виконати ідентифікацію та аутентифікацію на ранній стадії сеансу роботи користувача.

Друга проблема пов'язана з реалізацією захисту від завантаження несанкціонованих копій ОС. Для вирішення даного завдання зазвичай використовують тонкощі обробки завантаження з зовнішніх носіїв або перетворять (наприклад, шифрують) інформації на незнімних носіях комп'ютера.

У першому випадку завантаження з зовнішніх носіїв операційної системи неможлива фізично, у другому - навіть при успішному завантаженні з несанкціонованою копії ОС інформація недоступна.

Третя проблема пов'язана з формуванням завантажувальних носіїв (наприклад, дискет), що мають нестандартний вид, для їх спеціального використання.

Вирішення зазначених проблем зводиться в загальному випадку до програмування модифікованого завантажувача (або завантажувачів) операційної системи. Для простоти розглянемо технологію створення модифікованого завантажувача для гнучкого магнітного диска.

Розглянемо процес завантаження ОС для комп'ютерів сімейства Intel.

Після виконання всіх процедур, реалізованих в основному і розширених Bios, зчитується сектор з номером 1 з нульовою доріжкою поверхні читання в дисководі A або при його відсутності - з дисковода 80h (в разі якщо в установці Setup встановлена послідовність A :, C :). Лічені код розміром 512 байт завантажує його з адреси 0: 7C00h в оперативну пам'ять, після чого управління передається на цю адресу. На дискеті в цьому місці знаходиться програма початкового завантаження (BOOT-сектор), яка завантажує в пам'ять драйвери DOS і передає їм управління. На нульовій доріжці дискети також знаходяться системні області File Allocation Table і Root Directory, які формують файлову структуру дискети.

На жорсткому диску в першому секторі розміщується Master Root Record, який адресує виконання (по тій же схемі) активного завантажувача операційної середовища.

Таким чином, очевидно, що для модифікації завантажувача необхідно в загальному випадку виконати наступні операції:

- замістити первинний код завантажувача власним фрагментом;
- зберегти вихідний код завантажувального сектора (в разі необхідності його виконання);
- з урахуванням необхідності розміщення первинного завантажника за тією ж адресою, що і модифікованого, забезпечити коректне переміщення модифікованого завантажувача в іншу область пам'яті без втрати управління.

Отже, необхідно розмістити модифікований завантажувальний сектор на місці первинного (вихідного) завантажувача і розмістити первинний завантажувач (можливо, в перетвореному вигляді) в такому місці дискети або жорсткого диска, де буде забезпечена його гарантоване збереження.

Для дискети пропонується такий спосіб. Нульова доріжка дискети цілком копіюється на місце k-й доріжки. Вихідна нульова доріжка заповнюється нулями (або модифікується якось інакше для отримання потрібного виду дискети). На місце завантажувального сектора встановлюється необхідна програма.

Пропонований спосіб дозволяє виключити використання виготовленої дискети без завантаження з неї. Доповнивши DOS програмами перевірки цілісності, можна домогтися дотримання всіх вимог ізольованості програмно-апаратної середовища.

3.2 Дослідження програмного забезпечення системи захисту.

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів - універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки - обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

Рис.1. Типи програмних засобів захисту

Програмні засоби захисту інформації:

• Антивірусна програма (антивірус) - програма для виявлення комп'ютерних вірусів і лікування інфікованих файлів, а також для профілактики - запобігання зараженню файлів або операційної системи шкідливим кодом.

Для захисту від вірусів використовують три групи методів:

1. Методи, засновані на аналізі вмісту файлів (як файлів даних, так і файлів з кодами команд). До цієї групи належать сканування сигнатур вірусів, а також перевірка цілісності і сканування підозрілих команд.

2. Методи, засновані на відстежуванні поведінки програм при їх виконанні. Ці методи полягають в протоколюванні всіх подій, які загрожують безпеці системи і що відбуваються або при реальному виконанні перевіряється коду, або при його програмної емуляції.

3. Методи регламентації порядку роботи з файлами і програмами. Ці методи відносяться до адміністративних заходів забезпечення безпеки.

Метод сканування сигнатур (сигнатурний аналіз, сигнатурний метод) заснований на пошуку в файлах унікальною послідовності байтів - сигнатури,

характерної для певного вірусу. Для кожного знову виявленого вірусу фахівцями антивірусної лабораторії виконується аналіз коду, на підставі якого визначається його сигнатура. Отриманий кодовий фрагмент поміщають в спеціальну базу даних вірусних сигнатур, з якої працює антивірусна програма. Перевагою даного методу є відносно низька частка помилкових спрацьовувань, а головним недоліком - принципова неможливість виявлення в системі нового вірусу, для якого відсутня сигнатура в базі даних антивірусної програми, тому потрібно своєчасна актуалізація бази даних сигнатур.

Метод контролю цілісності ґрунтується на тому, що будь-яка несподівана і безпричинна зміна даних на диску є підозрілим подією, що потребує особливої уваги антивірусної системи. Вірус обов'язково залишає свідоцтва свого перебування (зміна даних існуючих (особливо системних або виконуваних) файлів, поява нових виконуваних файлів і т. Д.). Факт зміни даних - порушення цілісності - легко встановлюється шляхом порівняння контрольної суми (дайджесту), заздалегідь підрахованої для вихідного стану тестованого коду, і контрольної суми (дайджесту) поточного стану тестованого коду. Якщо вони не збігаються, значить, цілісність порушена і є всі підстави провести для цього коду додаткову перевірку, наприклад, шляхом сканування вірусних сигнатур. Зазначений метод працює швидше методу сканування сигнатур, оскільки підрахунок контрольних сум вимагає менше обчислень, ніж операції побайтового порівняння кодових фрагментів, крім того він дозволяє виявляти сліди діяльності будь-яких, в тому числі невідомих, вірусів, для яких в базі даних ще немає сигнатур.

Метод сканування підозрілих команд (евристичне сканування, евристичний метод) заснований на виявленні в сканованому файлі деякого числа підозрілих команд і (або) ознак підозрілих кодових послідовностей (наприклад, команда форматування жорсткого диска або функція впровадження в виконується процес або виконуваний код). Після цього робиться припущення про шкідливої суті файлу і робляться додаткові дії по його перевірці. Цей метод має гарний швидкодією, але досить часто він не здатний виявляти нові віруси.

Метод відстеження поведінки програм принципово відрізняється від методів сканування вмісту файлів, згаданих раніше. Цей метод заснований на аналізі поведінки запущених програм, який можна порівняти з затриманням злочинця «за руку» на місці злочину. Антивірусні засоби даного типу часто вимагають активної участі користувача, покликаного приймати рішення у відповідь на численні попередження системи, значна частина яких може виявитися згодом помилковими тривогами. Частота помилкових спрацьовувань (підозра на вірус для нешкідливого файлу або пропуск шкідливого файлу) при перевищенні певного порогу робить цей метод неефективним, а користувач може перестати реагувати на попередження або вибрати оптимістичну стратегію (дозволяти всі дії всіх запускаються програмами або відключити цю функцію антивірусного засобу). При використанні антивірусних систем, які аналізують поведінку програм, завжди існує ризик виконання команд вірусного коду, які могли б зашкодити захищається комп'ютера або мережі. Для усунення такої вади пізніше був розроблений метод емуляції (імітації), що дозволяє запускати тестовану програму в штучно створеної (віртуальної) середовищі, яку часто називають пісочницею (sandbox), без небезпеки пошкодження інформаційного оточення. Використання методів аналізу поведінки програм показало їх високу ефективність при виявленні як відомих, так і невідомих шкідливих програм.

Мною було проведено серію тестів антивірусних рішень, призначених для захисту системи. Антивіруси були перевірені на захист від новітніх та поширених загроз, помилкові спрацьовування і вплив на продуктивність комп'ютера.

Захист (Protection)

Одна з найважливіших категорій оцінки, які були використані при тестуванні антивірусів - захист. Методика включає тести, які задіють усі захисні компоненти і можливості антивірусу.

Продуктивність (Performance)

За допомогою даного параметра оцінюють вплив антивірусних рішень на системне швидкодію при виконанні основних повсякденних завдань на комп'ютері.

Зручність використання (Usability)

Цей критерій використовується для оцінки зручності використання антивірусного рішення, що представляє собою тестування на помилкові спрацьовування.

Антивірус	Захист	Продуктивність	Зручність використання	Загально
Avast Internet Security	6.0/6	5.5/6	6.0/6	**17.5**
AVG Internet Security	6.0/6	5.5/6	6.0/6	**17.5**
Kaspersky Internet Security	6.0/6	6.0/6	6.0/6	**18.0**
McAfee Total Protection	6.0/6	6.0/6	6.0/6	**18.0**
Cylance Smart Antivirus	2.5/6	6.0/6	4.0/6	**12.5**
ESET Internet Security	6.0/6	5.5/6	6.0/6	**17.5**
Malwarebytes Incident Response	5.5/6	4.5/6	4.5/6	**14.5**

Таблиця 1. Порівняння антивірусів

Після проведення тестування можна сказати, що антивірусні програми, що набрали 17.5-18 балів можна вважати найкращими для захисту та використання для захисту системи.

Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби. Крім програм шифрування і криптографічних систем, існує багато інших доступних зовнішніх засобів захисту інформації.

- Міжмережеві екрани (також звані брандмауерами або firewall). Між локальної та глобальної мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь проходить через них трафік мережевого /

транспортного рівнів. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю. Більш захищена різновид методу - це спосіб маскараду (masquerading), коли весь вихідний з локальної мережі трафік посилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.

Апаратний міжмережевий екран	**Програмний міжмережевий екран**
Відносна простота розгортання і використання	Можливість захисту мережі зсередини
Розміри і енергоспоживання	Можливість розмежування сегментів локальної мережі без виділення підмереж
Продуктивність	Можливість розгортання на існуючих серверах
Надійність	Розширений функціонал

Таблиця 2. Переваги міжмережевих екранів

Виходячи з вищеперерахованих переваг, я надаю перевагу апаратному міжмережевому екрану. Головними характеристиками, через які я обрав апаратний захист, є надійність та продуктивність, що необхідно для найкращого захисту системи.

- Proxy-servers (proxy - довіреність, довірена особа). Весь трафік мережевого / транспортного рівнів між локальної та глобальної мережами забороняється повністю - маршрутизація як така відсутня, а звернення з локальної мережі в глобальну відбуваються через спеціальні сервери-посередники. Очевидно, що при цьому звернення з глобальної мережі в локальну стають неможливими в принципі. Цей метод не дає достатнього захисту проти атак на більш високих рівнях - наприклад, на рівні додатку.
- VPN (віртуальна приватна мережа) дозволяє передавати секретну інформацію через мережі, в яких можливе прослуховування трафіку сторонніми людьми. Використовувані технології: PPTP, PPPoE, IPSec.

У наведеній нижче таблиці вказані технології шифрування, які використовує кожен з VPN-сервісів.

Продукт	OpenVPN	IKEv2/IPSec	L2TP/IPSec	PPTP	SSTP	SSH
Avast SecureLine VPN	+	-	-	-	-	-
AVG Secure VPN	+	-	-	-	-	-
CyberGhost VPN	+	+	+	+	-	-
hide.me VPN	+	+	-	-	+	-
Kaspersky Secure Connection	+	+	+	+	-	-
TorGuard	+	+	+	+	+	+
ZenMate VPN	+	+	+	-	-	-

Таблиця 3. Технології шифрування

VPN-сервіси використовуються для організації безпечного зашифрованого підключення до мережі Інтернет. Дані продукти популярні серед користувачів, який піклуються про конфіденційність своїх даних в Інтернеті. Серед недоліків VPN зазвичай відзначають зниження швидкості підключення. Було проведено тести швидкості та нижче наведені відсотки зниження швидкості через VPN.

	Відсоток зміни швидкості завантаження	**Відсоток зміни швидкості вивантаження**	**Відсоток зміни часу затримки**
	менше – краще	менше – краще	менше – краще
Mullvad VPN	19.0%	47.0%	33.3%
IVPN	22.6%	27.1%	71.4%
Mozila VPN	26.5%	20.9%	57.1%
NordVPN	28.7%	24.2%	0.0%
Hotspot Shield VPN	31.3%	60.0%	42.9%
TunnelBear VPN	46.6%	57.1%	100%
Proton VPN	72.7%	81.6%	77.8%
Середній результат	**28.7%**	**47%**	**57.1%**

Таблиця 4. Відсоток зниження швидкості

Типи програм для несанкціонованого доступу до даних.

Програми для запобігання несанкціонованому доступу до конфіденційної інформації умовно можна розділити на три типи:

- програми, шифрувальні інформацію;
- програми, що приховують інформацію;
- програми, які не шифрувальні інформацію, але блокують несанкціонований доступ або обмежують доступ до даних.

На практиці багато програм можуть одночасно ставитися до різних типів. Наприклад, деякі програми, які не шифрувальні інформацію, але блокують несанкціонований доступ до неї, можуть також приховувати цю інформацію на жорсткому диску, щоб відповідні файли або папки не відображалися в провіднику.

Програми для шифрування даних.

Програми, що дозволяють шифрувати інформацію, можна умовно розділити на два типи:

- програми, що реалізують симетричне шифрування, тобто шифрування з використанням одного і того ж ключа для шифрування і розшифрування інформації;
- програми, що реалізують асиметричне шифрування на основі пари ключів, один з яких, званий публічним, або відкритим (public), застосовується для шифрування, а другий, званий секретним, або приватним (private), - для розшифровки.

Відкритий і секретний ключі утворюють унікальну пару і пов'язані один з одним математично. Ідея полягає в тому, що, знаючи відкритий ключ, принципово неможливо обчислити секретний ключ.

Як правило, програми, що реалізують асиметричне шифрування на основі пари ключів, застосовуються не для зберігання інформації, а для безпечного пересилання даних через Інтернет. Наприклад, якщо потрібно, щоб вам переслали інформацію в зашифрованому вигляді, ви генеруєте пару ключів і пересилаєте відкритий ключ вашому кореспондентові. Ваш кореспондент,

використовуючи ваш відкритий ключ, зашифровує інформацію і пересилає її вам. Цю зашифровану інформацію можна розшифрувати тільки за допомогою секретного ключа, який зберігається у вас і утворює пару з відкритим ключем, з використанням якого була зашифрована інформація.

Якщо ж шифрування інформації необхідно лише для її безпечного зберігання, то краще застосовувати симетричне шифрування даних за допомогою одного-єдиного ключа. Потрібно відзначити, що деякі програми дозволяють генерувати ключі шифрування і згодом зберігати їх. При цьому передбачається, що ключ буде зберігатися на зовнішньому носії, наприклад на USB-флешці. Запам'ятати ключ нереально. Довжина ключа в багатьох алгоритмах шифрування становить 256 біт, і навіть якщо записати його в шістнадцятковому форматі, то запам'ятати його неможливо. Якщо ключ не передбачається зберігати окремо, то можна задати для нього пароль. Сам по собі пароль не є ключем шифрування, однак, використовуючи спеціальний алгоритм хешування, пароль завжди можна перетворити в потрібний ключ. Хешування, або знаходження хеш-функції, - це математична однонаправлена процедура перетворення пароля в комбінацію біт фіксованої довжини. Знаючи хеш-функцію пароля, принципово неможливо обчислити пароль - в цьому і полягає сенс односпрямованого перетворення.

Існує досить багато різних алгоритмів шифрування, і багато програм дозволяють вибирати алгоритм шифрування. Найбільш популярним зараз є алгоритм шифрування AES з довжиною ключа 256 біт. В принципі, підтримку програмою безлічі алгоритмів шифрування навряд чи можна розглядати як її перевага. Цілком достатньо, щоб програма підтримувала всього один криптостійкий алгоритм шифрування, наприклад AES з довжиною ключа 256 біт. Розкрити такий шифр, тобто підібрати ключ до нього, не представляється можливим. Дійсно, якщо довжина ключа становить 256 біт, то всього існує 2256 = 1,15792 · 1077 різних комбінацій ключів. Якщо використовувати метод перебору ключів і для простоти припустити, що комп'ютер в змозі перебирати мільйон ключів в секунду (хоча реальна швидкість перебору ключів для

сучасних ПК набагато нижче), то для перебору всіх ключів потрібно 3,78 · 1 063 років. Для довідки зазначимо, що вік нашого Всесвіту оцінюється всього в 14 млрд років. Навіть якщо припустити, що для перебору ключів буде застосовуватися який-небудь суперкомп'ютер, що дозволяє перебирати мільярди ключів в секунду, все одно завдання перебору всіх ключів буде нездійсненним. Так що сучасні методи шифрування забезпечують дуже надійний захист даних і навіть якщо зашифрована інформація потрапить до чужих рук, то хвилюватися, що хтось зможе отримати доступ до неї, немає причин. Це тільки у фільмах співробітники спецорганів в лічені хвилини підбирають ключі до шифрів - в житті все не так просто.

Програми, що приховують дані.

Програми для приховування даних просто приховують наявність даних на комп'ютері, так що за допомогою традиційних способів доступу їх виявити не можна. Доступ до даних можна отримати тільки при запуску спеціальної утиліти, але для цього необхідно знати пароль.

Програми, які блокують або обмежують доступ до даних.

Деякі програми дозволяють блокувати доступ до інформації без шифрування самих даних. Тобто передбачається, що для отримання доступу до даних (відкриття файлу) необхідно знати пароль. Крім того, такі програми, як правило, не тільки блокують доступ до даних, але і обмежують доступ до них. Наприклад, дозволяють встановити режим доступу «Тільки читання», тобто режим доступу без права внесення змін до документа і т.п.

Переваги та недоліки різних програм.

Програми, які блокують або обмежують доступ до даних, так само як і програми, що приховують інформацію, не можна вважати абсолютно надійними. У той же час вони дозволяють працювати з даними дуже швидко, що є їх незаперечною перевагою. Програми, в яких застосовуються криптографічні методи захисту, тобто шифрування даних, гарантують високу надійність, але процес шифрування і розшифровки вимагає часу і швидкість його виконання залежить від обчислювальної потужності комп'ютера.

3.3 Дослідження системи.

Для проведення класифікації ІСПД, визначення категорій персональних даних та експертної оцінки загрози їхній безпеці доцільно сформувати комісію із залученням фахівців в області інформаційної безпеки, в тому числі щодо захисту державної таємниці (особи з вищою профільною освітою в сфері захисту інформації або з підвищенням кваліфікації у сфері ЗІ).

Класифікація ІСПД здійснюється в залежності від категорії персональних даних (ПД), що не містять відомості, що відносяться до державної таємниці:

категорія 1 - ПД, що стосуються расової, національної приналежності, політичних поглядів, релігійних і філософських переконань, стану здоров'я, інтимного життя;

категорія 2 - ПД, що дозволяють ідентифікувати суб'єкта персональних даних і отримати про нього додаткову інформацію, за винятком ПД, що відносяться до категорії 1;

категорія 3 - ПД, що дозволяють ідентифікувати суб'єкта персональних даних;

категорія 4 - знеособлені і (або) загальнодоступні персональні дані.

Типові ІСПД, для яких порушення заданої характеристики безпеки персональних даних, які обробляються в них, може призвести до значних негативних наслідків для суб'єктів персональних даних, відносяться до класу 1 (К1), до негативних наслідків - до класу 2 (К2), до незначних негативних наслідків - до класу 3 (К3), не призводить до негативних наслідків для суб'єктів персональних даних - до класу 4 (К4).

При обробці персональних даних в інформаційній системі повинно бути забезпечено:

а) проведення заходів, спрямованих на запобігання несанкціонованого доступу до персональних даних та (або) передачі їх особам, які не мають права доступу до такої інформації (перш за все, регламентування доступу

співробітників до обробки персональних даних, парольний і антивірусний захист);

б) своєчасне виявлення фактів несанкціонованого доступу до персональних даних (перш за все, регламентування використання і регулярне оновлення антивірусних засобів);

в) недопущення впливу на технічні засоби автоматизованої обробки персональних даних, в результаті якого може бути порушено їх функціонування (охорона і регламентування використання технічних засобів);

г) можливість негайного відновлення персональних даних, модифікованих або знищених внаслідок несанкціонованого доступу до них (перш за все, шляхом зберігання резервних копій на знімних маркованих носіях);

д) постійний контроль за забезпеченням рівня захищеності персональних даних (здійснюваний в основному адміністраторами ІСПД і іншим персоналом).

Вибір типової моделі загроз здійснюється в залежності від того, чи мають ІСПД підключення до мереж загального користування та (або) мереж міжнародного інформаційного обміну, а також від їх структури (автономні автоматизовані робочі місця, локальні мережі, розподілені ІСПД з віддаленим доступом).

Найменша кількість загроз мають автоматизовані робочі місця і локальні ІСПД, не підключені до мереж загального користування. Якщо ІСПД нерозподілені і відповідають класу К3, то необхідні заходи щодо захисту персональних даних можуть бути здійснені без залучення фахівців в області інформаційної безпеки.

Для кожної загрози, наведеної в типової моделі, слід оцінити можливу ступінь її реалізації. Якщо вона виявиться високою, то це може зажадати застосування відповідних додаткових технічних засобів захисту інформації.

Можливість реалізації загрози залежить від вихідної захищеності ІСПД і ймовірності реалізації загрози.

Імовірність реалізації загрози - визначається експертним шляхом показник, що характеризує, наскільки вірогідною є реалізація конкретної загрози безпеки ПД для кожної ІСПД:

малоймовірно - відсутні об'єктивні передумови для створення іншої загрози (наприклад, відсутнє фізичне підключення до мережі);

низька ймовірність - об'єктивні передумови для реалізації загрози існують, але вжиті заходи істотно ускладнюють її реалізацію (наприклад, дії персоналу обумовлені в затвердженому регламенті або є засоби захисту та інструкції щодо їх застосування);

середня ймовірність - об'єктивні передумови для реалізації загрози існують, але вжиті заходи забезпечення безпеки ПД недостатні (наприклад, засоби захисту є, але інструкції щодо їх застосування відсутні);

висока ймовірність - об'єктивні передумови для реалізації загрози існують і заходи щодо забезпечення безпеки ПД не прийняті.

Зараз більш детально поговоримо про інструкцію по проведенню моніторингу інформаційної безпеки і антивірусного контролю при обробці персональних даних. Контроль за системою також є дуже важливою складовою в забезпеченні цілісності та конфіденційності даних.

1. Загальні положення, що визначають предмет інструкції, наприклад:

Порядок планування та проведення моніторингу інформаційної безпеки автоматизованих систем, що обробляють персональні дані, від несанкціонованого доступу, поширення, спотворення і втрати інформації установи.

2. Моніторинг апаратного забезпечення, наприклад: Моніторинг працездатності апаратних компонент автоматизованих систем, що обробляють персональні дані, здійснюється в процесі їх адміністрування і при проведенні робіт з технічного обслуговування обладнання. Найбільш суттєві компоненти системи, що мають вбудовані засоби контролю працездатності (сервери, активне мережеве обладнання) повинні контролюватися постійно в рамках роботи адміністраторів відповідних систем.

3. Моніторинг пральний захисту, наприклад:

Моніторинг пральний захисту і контроль надійності призначених для користувача паролів передбачають:

- встановлення термінів дії паролів (не більше 3 місяців);
- періодичну (не рідше 1 разу на місяць) перевірку користувальницьких паролів на кількість символів і очевидність з метою виявлення слабких паролів, які легко вгадати або дешифрувати за допомогою спеціалізованих програмних засобів (зломщиків паролів).

4. Моніторинг цілісності, наприклад:

Моніторинг цілісності програмного забезпечення включає наступні дії:

- перевірка контрольних сум і цифрових підписів каталогів і файлів сертифікованих програмних засобів при завантаженні операційної системи;
- виявлення дублікатів ідентифікаторів користувачів;
- відновлення системних файлів адміністраторами систем з резервних копій при розбіжності контрольних сум.

5. Моніторинг спроб несанкціонованого доступу, наприклад:

Попередження і своєчасне виявлення спроб несанкціонованого доступу здійснюється з використанням коштів операційної системи і спеціальних програмних засобів і передбачає:

- фіксацію невдалих спроб входу в систему в системному журналі;
- протоколювання роботи мережевих сервісів;
- виявлення фактів сканування певного діапазону мережевих портів в короткі проміжки часу з метою виявлення мережевих аналізаторів, які вивчають систему і виявляють її уразливості.

6. Моніторинг продуктивності, наприклад:

Моніторинг продуктивності автоматизованих систем, що обробляють персональні дані, проводиться за зверненнями користувачів, в ході адміністрування систем і проведення профілактичних робіт для виявлення спроб несанкціонованого доступу, які спричинили істотне зменшення продуктивності систем.

7. Системний аудит, наприклад:

Системний аудит проводиться щоквартально і в особливих ситуаціях. Він включає проведення оглядів безпеки, тестування системи, контроль внесення змін до системне програмне забезпечення.

Огляди безпеки проводяться з метою перевірки відповідності поточного стану систем, що обробляють персональні дані, рівню безпеки, що задовольняє вимогам політики безпеки. Огляди безпеки мають на меті виявлення всіх невідповідностей між поточним станом системи і станом, відповідному спеціально складеним списком для перевірки.

Огляди безпеки повинні включати:

звіти про безпеку для користувача ресурсів, що включають наявність повторюваних користувальницьких імен і ідентифікаторів, неправильних форматів реєстраційних записів, користувачів без пароля, неправильної установки домашніх каталогів користувачів і вразливостей для користувача оточень;

- перевірку вмісту файлів конфігурації на відповідність списку для перевірки;
- виявлення змін системних файлів з часу проведення останньої перевірки (контроль цілісності системних файлів);
- перевірку прав доступу та інших атрибутів системних файлів (команд, утиліт і таблиць);
- перевірку правильності настройки механізмів аутентифікації і авторизації мережевих сервісів;
- перевірку коректності конфігурації системних і активних мережевих пристроїв (мостів, маршрутизаторів, концентраторів і мережевих екранів).

Активне тестування надійності механізмів контролю доступу проводиться шляхом здійснення спроб проникнення в систему (за допомогою автоматичного інструментарію або вручну).

Пасивне тестування механізмів контролю доступу здійснюється шляхом аналізу конфігураційних файлів системи. Інформація про відомих вразливості

витягується з документації і зовнішніх джерел. Потім здійснюється перевірка конфігурації системи з метою виявлення небезпечних станів системи(тобто таких станів, в яких можуть проявляти себе відомі уразливості). Якщо система знаходиться в небезпечному стані, то з метою нейтралізації вразливостей необхідно або змінити конфігурацію системи (для ліквідації умов прояви уразливості), або встановити програмні корекції, або встановити інші версії програм, в яких дана уразливість відсутня, або відмовитися від використання системного сервісу, що містить дану уразливість.

Внесення змін до системне програмне забезпечення здійснюється адміністраторами систем, що обробляють персональні дані, з обов'язковим документуванням змін у відповідному журналі; повідомленням кожного співробітника, якого стосується зміна; вислуховування претензій в разі, якщо ця зміна заподіяло кому-небудь шкоду; розробкою планів дій в аварійних ситуаціях для відновлення працездатності системи, якщо внесена в неї зміна вивело її з ладу.

8. Антивірусний контроль, наприклад:

Для захисту серверів і робочих станцій необхідно використовувати антивірусні програми:

- резидентні антивірусні монітори, які контролюють підозрілі дії програм;
- утиліти для виявлення і аналізу нових вірусів.

До використання допускаються тільки ліцензійні засоби захисту від шкідливих програм і вірусів або сертифіковані вільно поширювані антивірусні засоби.

При підозрі на наявність невиявлених встановленими засобами захисту заражень слід використовувати Live CD з іншими антивірусними засобами.

Установка і настройка засобів захисту від шкідливих програм і вірусів на робочих станціях і серверах автоматизованих систем, що обробляють персональні дані, здійснюється адміністраторами відповідних систем відповідно до посібників по установці придбаних засобів захисту.

Встановлюється (змінюване) програмне забезпечення повинне бути попередньо перевірено адміністратором системи на відсутність шкідливих програм і комп'ютерних вірусів. Безпосередньо після установки (зміни) програмного забезпечення робочої станції повинна бути виконана антивірусна перевірка.

Запуск антивірусних програм повинен здійснюватися автоматично за завданням, централізовано створеному з використанням планувальника завдань (що входять в поставку операційної системи або поставляється разом з антивірусними програмами).

Антивірусний контроль робочих станцій повинен проводитися щодня в автоматичному режимі. Якщо перевірка всіх файлів на дисках робочих станціях займає неприйнятно великий час, то допускається проводити вибіркову перевірку завантажувальних областей дисків, оперативної пам'яті, критично важливих інстальованих файлів операційної системи і завантаження по мережі або з зовнішніх носіїв. У цьому випадку повна перевірка повинна здійснюватися не рідше одного разу на тиждень в період неактивності користувача. Користувачам рекомендується здійснювати повну перевірку під час перерви на обід шляхом перекладу робочої станції до відповідного автоматичний режим функціонування в замкненому приміщенні.

Обов'язковому антивірусного контролю підлягає будь-яка інформація (виконувані файли, текстові файли будь-яких форматів, файли даних), що отримується користувачем по мережі або завантажується з знімних носіїв (магнітних дисків, оптичних дисків, флеш-накопичувачів і т.п.). Контроль інформації повинен проводитися антивірусними засобами в процесі або відразу після її завантаження на робочу станцію користувача. Файли, що поміщаються в електронний архів, повинні в обов'язковому порядку проходити антивірусний контроль.

Встановлюється (змінюване) на сервери програмне забезпечення повинно бути попередньо перевірено адміністратором системи на відсутність комп'ютерних вірусів і шкідливих програм. Безпосередньо після установки

(зміни) програмного забезпечення сервера повинна бути виконана антивірусна перевірка.

На серверах систем, що обробляють персональні дані, необхідно застосовувати спеціальне антивірусне програмне забезпечення, що дозволяє:

- здійснювати антивірусну перевірку файлів в момент спроби запису файлу на сервер;
- перевіряти каталоги і файли за розкладом з урахуванням навантаження на сервер.

На серверах електронної пошти необхідно застосовувати антивірусне програмне забезпечення, що забезпечує перевірку всіх вхідних повідомлень. У разі якщо перевірка вхідного повідомлення на поштовому сервері показала наявність в ньому вірусу або шкідливого коду, відправка даного повідомлення повинна блокуватися. При цьому повинно здійснюватися автоматичне оповіщення адміністратора поштового сервера, відправника повідомлення і адресата.

Необхідно організувати регулярне оновлення антивірусних баз на всіх робочих станціях і серверах.

Адміністратори систем повинні проводити регулярні перевірки протоколів роботи антивірусних програм з метою виявлення користувачів і каналів, через яких поширюються віруси. При виявленні заражених вірусом файлів адміністратор системи повинен виконати наступні дії:

- відключити від комп'ютерної мережі робочі станції, що представляють вірусну небезпеку, до повного з'ясування каналів проникнення вірусів і їх знищення;
- негайно повідомити про факт виявлення вірусів безпосередньому начальнику із зазначенням можливого джерела (відправника, власника і т.п.) Зараженого файлу, типу зараженого файлу, характеру міститься в файлі інформації, типу вірусу і виконаних антивірусних заходів.

9. Аналіз інцидентів, наприклад:

Якщо адміністратор системи, що обробляє персональні дані, підозрює або отримав повідомлення про те, що його система піддається атаці або вже була скомпрометована, то він повинен встановити:

- факт спроби несанкціонованого доступу (НСД);
- чи продовжується НСД зараз;
- хто є джерелом НСД;
- що є об'єктом НСД;
- коли відбувалася спроба несанкціонованого доступу;
- як і за яких обставин була зроблена спроба несанкціонованого доступу;
- точка входу порушника в систему;
- чи була спроба НСД успішної;
- визначити системні ресурси, безпека яких була порушена;
- яка мотивація спроби несанкціонованого доступу.

Для виявлення спроби несанкціонованого доступу необхідно встановити, які користувачі в даний час працюють в системі, на яких робочих станціях. Виявити підозрілу активність користувачів, перевірити, що всі користувачі увійшли в систему зі своїх робочих місць і ніхто з них не працює в системі незвично довго. Крім того, необхідно перевірити, що ніхто з користувачів не виконує підозрілих програм і програм, що не відносяться до його сфери діяльності.

При аналізі системних журналів адміністратору необхідно провести наступні дії:

- перевірити наявність підозрілих записів системних журналів, зроблених в період передбачуваної спроби несанкціонованого доступу, включаючи вхід в систему користувачів, які повинні б були відсутні в цей період часу, входи в систему з несподіваних місць, в незвичайний час і на короткий період часу;
- перевірити не знищений чи системний журнал і чи немає в ньому прогалин;

- переглянути списки команд, виконаних користувачами в розглянутий період часу;
- перевірити наявність вихідних повідомлень електронної пошти, адресованих підозрілим хостам;
- перевірити наявність місць в журналах, які виглядають незвично;
- виявити спроби отримати повноваження суперкористувача або інший привілейований користувач;
- виявити наявність невдалих спроб входу в систему.

В ході аналізу журналів активного мережного обладнання (мостів, перемикачів, маршрутизаторів, шлюзів) необхідно:

- перевірити наявність підозрілих записів системних журналів, зроблених в період передбачуваної спроби несанкціонованого доступу;
- перевірити не знищений чи системний журнал і чи немає в ньому прогалин;
- перевірити наявність місць в журналах, які виглядають незвично;
- виявити спроби зміни таблиць маршрутизації і адресних таблиць;
- перевірити конфігурацію мережевих пристроїв з метою визначення можливості знаходження в системі програми, переглядає весь мережевий трафік.

Для виявлення в системі слідів, залишених зловмисником, у вигляді файлів, вірусів, троянських програм, зміни системної конфігурації необхідно:

- скласти базову схему того, як зазвичай виглядає система;
- провести пошук підозрілих файлів, прихованих файлів, імен файлів і каталогів, які зазвичай використовуються зловмисниками;
- перевірити вміст системних файлів, які зазвичай змінюються зловмисниками;
- перевірити цілісність системних програм;
- перевірити систему аутентифікації і авторизації.

У разі зараження значної кількості робочих станцій після усунення його наслідків проводиться системний аудит.

Особливості моніторингу інформаційної безпеки персональних даних в окремих автоматизованих системах можуть регулюватися додатковими інструкціями.

Однією з основних причин актуальності внутрішніх загроз інформаційної безпеки є несанкціонований витік інформації за межі захищених ІС, обсяг якого має стійку тенденцію до збільшення. Такі загрози можна мінімізувати шляхом впровадження систем протидії внутрішнім загрозам інформаційної безпеки. Всього існує чотири класи таких систем. До них відносяться системи моніторингу та аудиту, системи аутентифікації, інструменти шифрування та системи виявлення та запобігання витоку інформації.

Системи моніторингу та аудиту дозволяють записувати дії користувачів і процеси в ІР, включаючи дії і процеси, пов'язані з передачею даних за межі ІР по мережевих каналах. Такі системи є важливим інструментом в розслідуванні зафіксованих випадків несанкціонованого витоку інформації по периметру захищається ІР і проведенні їх аналізу. Недоліком таких систем є відсутність можливості запобігти несанкціонованій витік інформації. Робота систем моніторингу та аудиту не передбачає алгоритмів аналізу зафіксованих подій. Це означає, що вони не можуть визначити, чи прийнятна записане подія з точки зору інформаційної безпеки чи ні. Природно, що в таких системах не передбачені будь-які алгоритми блокування передачі даних по мережевих каналах.

Системи аутентифікації ІР-користувачів використовуються для захисту від несанкціонованого доступу до даних. В їх основі лежить процес аутентифікації користувача (може бути дво- або три етапним). В результаті користувачеві може бути надано доступ до запитаним ресурсів чи ні, що запобігає можливу несанкціоновану витік інформації за межі ІР. Такі інструменти можуть не захищати інформацію від користувача, який має доступ до даних у відповідності з політикою безпеки ІР, але планує використовувати її з метою, що суперечать чинному законодавству або політики безпеки компанії (від інсайдера).

Засоби шифрування носіїв змінюють дані таким чином, що їх можна використовувати без спеціальних програм (ключів). Цей клас програм захистить

дані від витоку в разі втрати мобільного системи для зберігання або обробки інформації і перехоплення даних зловмисником поза захищеного IP. Ефективність такого засобу захисту нівелюється, якщо разом з даними зловмисник отримує ключі шифрування.

Системи запобігання витоку даних (DLP) сканують можливі канали витоку даних в режимі реального часу і можуть відстежувати дії користувачів, а також процеси обробки і передачі інформації в ІС. У цьому випадку такі системи вміють розпізнавати інформацію за певними категоріями. Вони можуть бути складними або локальними.

Інтегровані DLP-системи контролюють кілька каналів витоку інформації. Наприклад, копіювання на мобільні носії, системи друку, мережеві канали передачі інформації і т. Д Локальні системи контролюють тільки один з можливих каналів витоку інформації, часто мережевий. Такі системи можуть бути оснащені проактивними технологіями, що дозволяють не тільки виявляти випадки несанкціонованого переміщення інформації по периметру захищається IP, а й блокувати їх. Додатковою функцією DLP-систем може бути шифрування даних під час запису на носій або файли. Існують і інші програмні та апаратні засоби захисту інформації від внутрішніх загроз інформаційної безпеки, які не можна безпосередньо віднести до вище перелічених категорій. Наприклад, засоби блокування зовнішніх носіїв. Такі системи не можуть розпізнавати інформацію за категоріями, які не відрізняти інформацію обмеженого поширення від загальної і є реалізацією окремих функцій наведених систем захисту від внутрішніх загроз. На сьогоднішній день тільки системи виявлення та запобігання витоку інформації (DLP-системи) є єдиним рішенням для запобігання витоку інформації в реальному часі за межі захищеного IP-простору на основі фільтрації даних або зовнішніх атрибутів, які супроводжують процес переміщення даних. Зазвичай ядром таких DLP-систем є технології категоризації контенту на основі контейнерного або контекстного аналізу вихідного потоку. До переваг контейнерного аналізу можна віднести простоту його реалізації, до недоліків - організаційні труднощі в реалізації і обмежені можливості контролю

вихідного трафіку. Контекстний аналіз в основному використовує лінгвістичні або статичні методи аналізу файлів.

Перейдемо безпосередньо до створення системи захисту персональних даних на підприємстві. Як уже було описано мною вище, загрози можуть бути різного характеру, такі як програмні атаки, спроби несанкціонованого доступу, фізичні загрози, природні. Мета нашої системи – передбачити та запобігти можливому витоку даних. Слід обрати програмне та апаратне забезпечення, яке б могло б забезпечити цілісність та конфіденційність інформації.

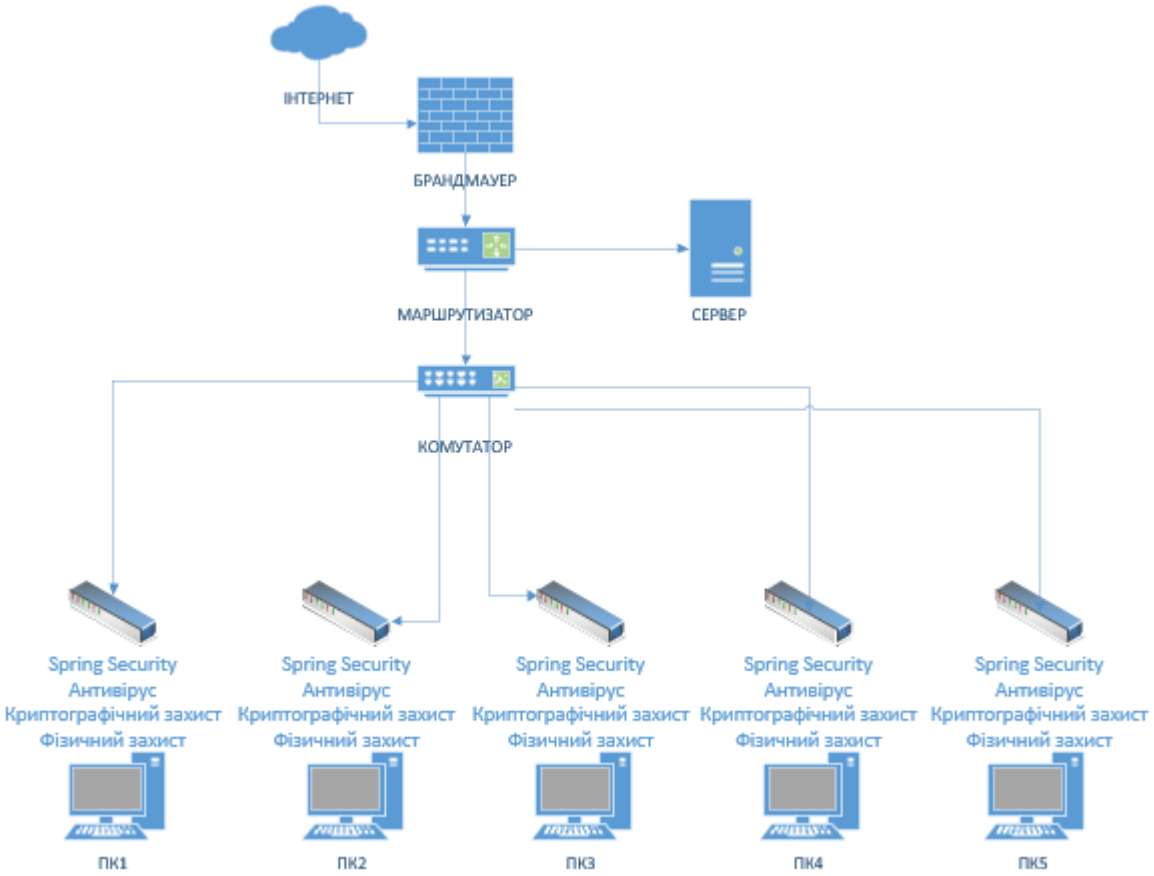


Рис.2. Схема системи захисту підприємства

Насамперед, слід створити систему авторизації / автентифікації, щоб зловмисники не могли просто отримати доступ до даних. До цієї інформації має мати доступ лише відділ, який займається обробкою та захистом цих даних. Одним з найкращих фреймворків для реалізації авторизації та автентифікації є Spring Security. Це потужна система, що легко конфігурується, для

автентифікації та контролю доступу. Це фактичний стандарт захисту програм на основі Spring. Spring Security - це структура, яка зосереджена на забезпеченні автентифікації та авторизації програм Java. Як і всі проекти Spring, справжня сила Spring Security полягає в тому, як легко її можна розширити, щоб задовольнити власні вимоги. Нижче представлена архітектура даного фреймворку.

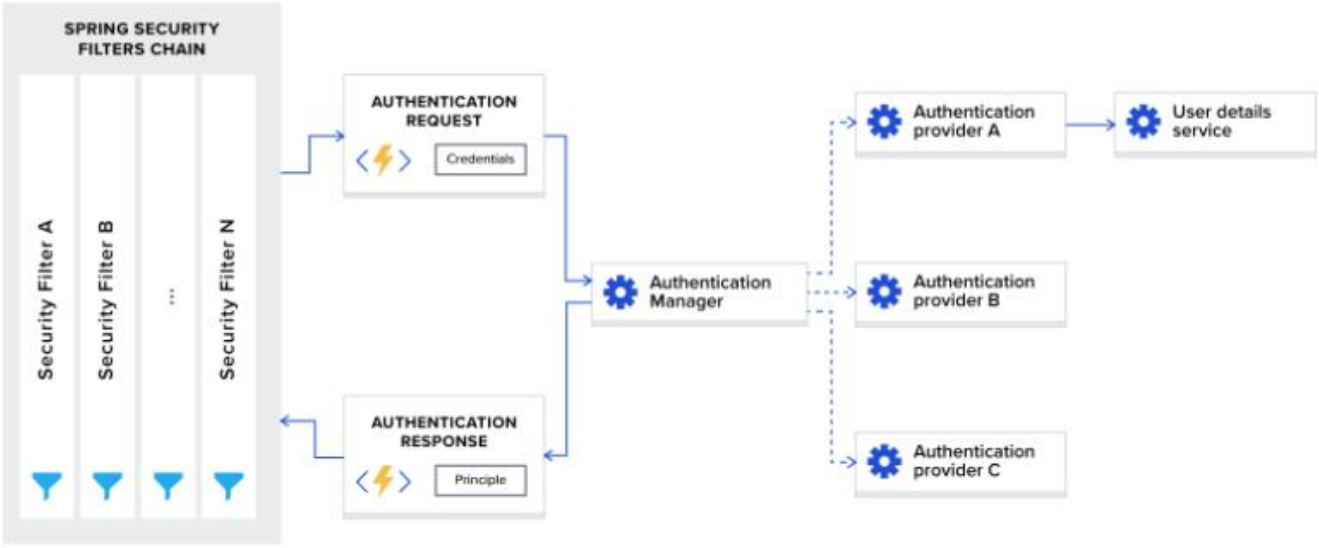


Рис.3. Принцип роботи Spring Security

Коли ви додаєте структуру Spring Security до своєї програми, вона автоматично реєструє ланцюжок фільтрів, який перехоплює всі вхідні запити. Цей ланцюжок складається з різних фільтрів, і кожен з них обробляє певний варіант використання.

Наприклад: Перевірте, чи є загальнодоступною доступна URL-адреса на основі конфігурації. У разі аутентифікації на основі сеансу перевірте, чи користувач вже автентифікований у поточному сеансі. Перевірте, чи користувач уповноважений виконувати запитувану дію тощо.

Однією важливою деталлю, яку слід зазначити, є те, що фільтри Spring Security реєструються з найнижчим порядком і є першими фільтрами, що викликаються. У деяких випадках використання, якщо ви хочете поставити власний фільтр перед ними, вам доведеться додати відступ до їх замовлення. Це можна зробити за такої конфігурації: spring.security.filter.order = 10. Щойно ми

додамо цю конфігурацію до нашого файлу application.properties, у нас буде місце для 10 спеціальних фільтрів перед фільтрами Spring Security.

Нижче наведена частина коду з налаштуванням доступу:

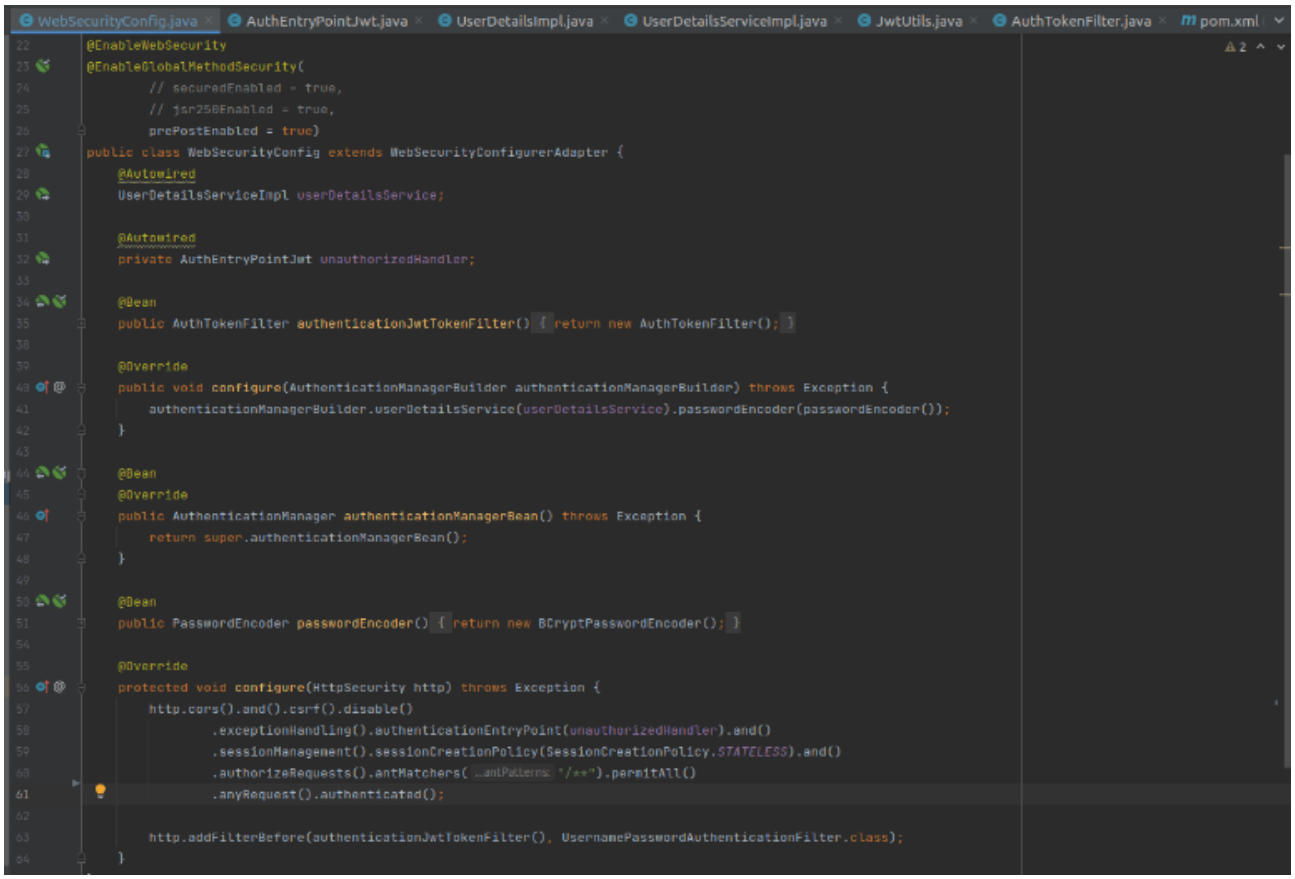


Рис.4. Налаштування доступу

Одним з найважливіших компонентів захищеної системи є міжмережевий екран. Для своєї системи я обрав екран Fortinet FGR30D. Зараз я хочу більш детально розповісти про нього та обґрунтувати свій вибір.

FortiGateRugged-30D – компактний пристрій безпеки в особливо міцному корпусі, розроблено спеціально для роботи в суворих умовах. Невеликий, легкий, але поєднує в собі весь функціонал класичного UTM пристрої від Fortinet. Система ліцензування "за пристрій" гарантує, що кількість користувачів обмежена тільки продуктивністю системи, що дозволяє економити на операційних витратах .

Можливості та переваги FortiGateRugged-30D:

- Повний функціонал безпеки - міжмережевий екран, система запобігання вторгнень, контроль додатків, VPN і веб-фільтрація.
- Компактний розмір і особливо міцний корпус, розроблений для роботи в промислових мережах і суворих умовах.
- Система ліцензування "за пристрій" гарантує, що кількість користувачів обмежена тільки продуктивністю системи, що дозволяє економити на операційних витратах.
- Простота налаштування і першого запуску пристрою.
- Автоматизоване оновлення підписок в режимі реального часу за допомогою сервісів підписки FortiGuard.

Ще одним дуже важливим фактором у захисті системи є біометричний захист. Системи біометричного захисту використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною аутентифікацією. Його суть – визначити, чи справді індивід є тією особою, якою він або вона себе називає. Це відрізняє аутентифікацію від ідентифікації та авторизації. Мета ідентифікації – перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а авторизація полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи. Для своєї системи я обрав захист ZKTECO INBIO260.

Функції:

- Доступ по відбитку пальця, безконтактної картки, коду;
- Вбудоване реле для управління електронними замками;
- Тимчасові зони для обмеження доступу згідно дозволених тимчасових інтервалів;
- Комбінації розблокування дверей;
- Вихід з приміщення за допомогою кнопки виходу;
- Вхід RS 485 для підключення біометричних зчитувачів;
- Вхід Wiegand для підключення зчитувачів rfid міток;
- Функції обліку робочого часу;

- Автономна пам'ять зберігання подій відвідуваності. Безкоштовна програма для обліку робочого часу співробітників;
- Функції інтелектуальної логіки роботи;
- Заборона подвійного проходу. Подвійний прохід заборонено без запису виходу;
- Логіка роботи шлюзових кабін- другі двері не відчиняться, поки не будуть закриті 1 двері;
- Режим вільного проходу в призначений час, після піднесення карти для розблокування;
- Функція "палець під примусом" - відкриття дверей і відправка сигналу тривоги;
- Багатофакторна доступність комбінації методів доступу.

Криптографічний захист (шифрування) інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства.

Для своєї системи я обрав термінал криптографічного захисту «ЛАВИНА-Е». Він забезпечує:

Прохідне шифрування трафіку IP-мереж.

Шифрування трафіку здійснюється на периметрі локальної мережі. Криптографічна обробка в режимі on-line забезпечує "прозору" роботу мережевих додатків обробки даних, IP-телефонії, відеоконференцзв’язку.

Віртуальні канали шифрованого зв’язку.

Під час обміну шифрованою інформацією створюються віртуальні канали шифрованого зв’язку за схемою, яка задається адміністратором комплексу.

Резервування каналів.

Для кожного напрямку зв’язку можуть бути визначені декілька віртуальних каналів з різними маршрутами, що забезпечує резервування каналів зв’язку.

Ключова система.

Ключова система забезпечує централізоване підготування та розподілення ключових даних. Під час генерації ключових даних пристроєм О372-Е використовуються фізичні сенсори, що відповідають FIPS 140-2. Розподілення здійснюється двома методами: передача мережею шифрованого зв'язку та/або на носіях ключових даних.

Апаратна реалізація криптомодуля.

Функції криптографічного перетворення здійснюються спеціалізованими мікросхемами із дублюванням, що забезпечує високу пропускну здатність та надійність шифрування.

Балансування завантаження каналів.

Віртуальні канали можуть об'єднуватися в групи, з метою балансування завантаження та збільшення пропускної здатності вузлів мережі.

Резервування обладнання.

Обладнання може дублюватися з метою "гарячого" резервування та аґреґування пропускної здатності.

Моніторинг та керування.

Моніторинг та керування обладнанням здійснюється як локально, так і віддалено, за допомогою централізованої системи керування ЦСК. Програмне забезпечення ЦСК встановлюється на комп'ютері під керуванням операційної системи Windows та дозволяє керувати режимами роботи обладнання, змінювати параметри конфігурації, переглядати статистичну інформацію, протоколювати та обробляти повідомлення про події в мережі шифрованого зв'язку. Захист від несанкціонованого доступу до керування обладнанням забезпечується за допомогою двофакторної аутентифікації.

Важливою складовою захисту від програмної атаки є антивірус. Антивірус – програмний засіб, призначений для боротьби з вірусами. Виходячи з визначення, основними завданнями антивірусу є:

- Перешкоджання проникненню вірусів у комп'ютерну систему;
- Виявлення наявності вірусів у комп'ютерній системі;

- Усунення вірусів з комп’ютерної системи без нанесення ушкоджень іншим об’єктам системи ;
- Мінімізація збитку від дій вірусів.

Для своєї системи я обрав AVG AntiVirus. Це антивірусне програмне забезпечення розроблене чеською компанією AVG Technologies (раніше відома під назвою Grisoft), підрозділом Avast Software. Програма доступна на платформах Microsoft Windows, OS X та Android. Антивірус має сканер файлів, має змогу перевіряти електронну пошту, та моніторинг системи. Програма містить пошуковий механізм Virus Stalker, яких сертифікований незалежними дослідницькими лабораторіями.

Комерційна версія ділить на два варіанта: AVG Antivirus Pro и AVG Internet Security. Остання додатково має інструменти запобігання та захисту від Інтернет-атак.

У якості VPN – серверу я обрав TorGuard. Його переваги - це потужний захист, вбудований блокувальник реклами, підтримка P2P, сувора безлоговая політика, чуйна техпідтримка, можливість впевнено обходити навіть найскладніші блокування доступу.

Не слід забувати про стихійні лиха та надзвичайні ситуації. Якщо інформація зберігається лише на комп’ютерах та серверах підприємства, то є великий ризик втратити їх у випадку пожежі або іншої ситуації. В такому випадку я радив би користуватися віддаленими фізичними серверами. Але у цьому випадку є ризик втрати цих даних саме з цих серверів. Тому слід забезпечувати захист і цих серверів також.

3.4 Висновки до третього розділу.

У даному розділі ми розглянули варіанти апаратного та програмного захисту систем захисту даних. Можна сказати, що є дуже багато засобів, для забезпечення безпеки персональної інформації, адже дана проблема є дуже

популярною. Тому багато компаній намагаються створювати програми та пристрої, щоб гарантувати надійність для своїх користувачів.

Мною було запропоновано створення системи, яка б захищала персональні данні від крадіжки. Для початку треба створити систему ідентифікації / автентифікації. Також для захищеності даних слід встановити необхідне захисне ПО, антивіруси, для запобігання втручання в систему за допомогою програм-вірусів. Слід встановити криптографічний захист, аби ці дані було складно розшифрувати. Також потрібно встановити біометричний захист для того, щоб не було фізичного втручання у систему.

ВИСНОВКИ

На сьогоднішній день, проблема захисту даних, як персональних, так і звичайних, є дуже поширеною. Насамперед, це популярне питання для державних установ та організацій, які своєю діяльністю узагальнюють та використовують інформацію про особу. У ході моєї дипломної роботи я описав проблеми загроз для систем захисту даних.

У ході проведеної мною роботи було виявлено ряд недоліків існуючих засобів, які використовуються для захисту персональних даних. Проаналізувавши інформаційну безпеку підприємства можна зробити висновок, що інформаційної безпеки приділяється недостатня увага: відсутність паролів доступу в систему; відсутність паролів при роботі програмою з 1С: підприємство, при зміні даних; відсутня додатковий захист файлів та інформації (відсутній елементарний запит пароля при відкритті або зміні інформації в файлах, не кажучи вже про кошти шифрування даних); нерегулярне оновлення баз програми антивіруса і сканування робочих станцій; велика кількість документів на паперових носіях в основному лежать в папках (іноді і без них) на робочому столі співробітника, що дозволяє зловмисникам без праці скористатися такого роду інформаціях в своїх цілях; не проводиться регулярне обговорення питань інформаційної безпеки на підприємстві і виникаючих проблем в цій галузі; не організована регулярна перевірка працездатності інформаційних систем підприємства, налагодження проводиться тільки в тому випадку, коли вони виходять з ладу; відсутність політики інформаційної безпеки; відсутність системного адміністратора. Все перераховане вище є дуже важливими недоліками забезпечення інформаційної безпеки підприємства.

Результатом виконаної роботи являються розроблена система захисту персональних даних на підприємстві. Під час виконання роботи було:

1. Проведено аналіз існуючих систем захисту персональних даних. Було виявлено їх переваги та недоліки. З часом з’являються все нові та нові

засоби викрадення персональних даних, тому систему захисту потрібно весь час покращувати та оновлювати.

2. Створено систему, що займається захистом персональних даних на підприємстві. Виходячи з першого завдання, було узято усі найкращі якості існуючих систем та сформовано надійну систему.

3. Дослідив створену систему. Описав та обґрунтував свій вибір програмного та апаратного забезпечення, з чого можна зробити висновок, що дана система є повністю надійною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Оніщенко О.В. Конституційне та адміністративне право / Оніщенко О.В. // Захист персональних даних. – 2012 – №1 – С. 60-63.

2. Про інформацію: Закон України від 02.10.1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст.650.

3. Конституція України. Прийнята на п‘ятій сесії Верховної Ради України 28.06.1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

4. Про захист персональних даних: Закон України від 01.06.2010 р. // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

5. Про ратифікацію Конвенції про захист осіб у зв‘язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв‘язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 06.07.2010 р. // Відомості Верховної Ради України. – 2010. – № 46. – Ст. 542.

6. Деякі питання практичного застосування Закону України «Про захист персональних даних: Роз’яснення Мінюсту від 21.12.2011 р. / [Електронний ресурс]. – Режим доступу: // http://zakon2.rada.gov.ua/laws/show/n0076323-1

7. Офіційний сайт Державної служби України з питань захисту персональних даних / [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/indexDovidkaInfo.html

8. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від 20.01.2012 р. / [Електронний ресурс]. – Режим доступу: http://www.ccu.gov.ua/uk/doccatalog/list?currDir=167724.

9. Кодекс законів про працю України від 10.12.1971 р. // Відомості Верховної Ради УРСР від 17.12.1971.

10. Цивільний кодекс України від 16.01.2003 р. // Голос України. – 2003. – № 47-с. 48.

11. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46ЕС Європейського Парламенту і Ради від 24.10.1995 / [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_242

12. Захист персональних даних на підприємстві [Електронний ресурс] / В. Мачуський – 2018. – Режим доступу: World Wide Web. – URL: https://www.businesslaw.org.ua/zahyst-personalnyx-danyx-na-pidpryemstvi/

13. Захист персональних даних [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://tzi.com.ua/zpd.html

14. Программно-аппаратная защита информации [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/programmno-apparatnaya/

15. Захист персональних даних: деякі практичні аспекти [Електронний ресурс] – 2011. – Режим доступу: World Wide Web. – URL: https://www.asterslaw.com/ua/press_center/news/personal_data_protection_some_practical_aspects/

16. Угрозы информационной безопасности [Електронний ресурс] – 2017. – Режим доступу: World Wide Web. – URL: https://www.anti-malware.ru/threats/information-security-threats

17. Збір персональних даних та інформаційна безпека [Електронний ресурс] / О. Зозуля – 2018. – Режим доступу: World Wide Web. – URL: https://uz.ligazakon.ua/ua/magazine_article/EA012189

18. Шифрование данных: как защитить самое ценное [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.sim-networks.com/blog/data-encryption-best-practices

19. М. А. Никитин, Д. А. Лютов / Организация работ по защите персональных данных – Самара, 2007. – 131 с.

20. Программно-аппаратная защита информации [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/programmno-apparatnaya/

21. Г.М. Гулак, В.А. Козачок, П.М. Складанний, М.О. Бондаренко, Б.В. Вовкотруб // Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. – 2017. – №2(30). – С. 65-70.

22. Программы для предотвращения несанкционированного доступа к информации [Електронний ресурс] – 2017. – Режим доступу: World Wide Web. – URL: https://compress.ru/article.aspx?id=18759

23. Зайцев А.П., Голубятников И.В. / Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. – М.: Машиностроение-1, 2001. − 126 с.

24. Сулавко, А. Е. Технологии защиты от внутренних угроз информационной безопасности [Текст] / А. Е. Сулавко // Вестник СибАД. — 2011. — № 1(19) — С. 45–51.

25. Коржов, В. В. Защита персональных данных: проблемы и пути решения [Текст] / В. В. Коржов // Открытые си стемы. — 2010. — № 10. — С. 11.

26. Марков, А. П. Проблемы и решения по защите персональ ных данных в информационных системах персональных данных [Текст] / А. П. Марков, Б. И. Сухинин // Компью терная безопасность. — 2009. — № 5. — С. 20–27.

27. Німченко, Т. В. Критерій визначення з переліку даних тих, що відносяться до категорії персональні [Текст] / Т. В. Нім ченко // Вісник інженерної академії України. — 2015. — № 1. —С. 199–202.

28. Філоненко, С. Ф. Система попередження витоку персональніх даних мережевими каналами [Текст] / С. Ф. Філоненко, І. М. Мужик, Т. В. Німченко //

Ukrainian Scientific Jornal of Information Security. — 2014. — Vol. 20, № 3. — P. 279–285.

29. Німченко, Т. В. Алгоритм виявлення несанкціонованого витоку персональних даних мережевими каналами [Текст] / Т. В. Німченко, І. М. Мужик, А. І. Мужик // Вісник інженрної академії України. — 2014. — № 3–4. — С. 199–203.

30. Гуцалюк, М. Інформаційна безпека України: нові загрози та організація протидії [Текст] / М. Гуцалюк // Правова інформатика. — 2004. — № 3. — С. 37–41.

Додаток А

Реалізація класу UserDetailsServiceImpl

```
import com.sirenko.diplom.Entity.User;
import com.sirenko.diplom.Repository.UserRepository;
import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.security.core.userdetails.UserDetails;
import org.springframework.security.core.userdetails.UserDetailsService;
import org.springframework.security.core.userdetails.UsernameNotFoundException;
import org.springframework.stereotype.Service;
import org.springframework.transaction.annotation.Transactional;

@Service
public class UserDetailsServiceImpl implements UserDetailsService {
    @Autowired
    UserRepository userRepository;


//    @Override
//    @Transactional
//    public UserDetails loadUserByEmail(String username) throws
UsernameNotFoundException {
//        //userDao.openCurrentSessionwithTransaction();
//
//        User user = userDao.findByEmail(username)
//                .orElseThrow(() -> new UsernameNotFoundException("User Not Found
with username: " + username));
//        System.out.println(user.getRoles().toString());
//        //userDao.closeCurrentSessionwithTransaction();
//        return UserDetailsImpl.build(user);
//    }

    @Override
    @Transactional
    public UserDetails loadUserByUsername(String username) throws
UsernameNotFoundException {
        //userDao.openCurrentSessionwithTransaction();

        User user = userRepository.findByName(username)
                .orElseThrow(() -> new UsernameNotFoundException("User Not Found
with username: " + username));
```

Продовження додатку А

```
        System.out.println(user.getRoles().toString());

        //userDao.closeCurrentSessionwithTransaction();
        return UserDetailsImpl.build(user);
    }


}
```

Додаток Б

Створення унікального токену розпізнавання клієнта

```
import com.sirenko.diplom.Security.services.UserDetailsImpl;
import io.jsonwebtoken.*;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import org.springframework.beans.factory.annotation.Value;
import org.springframework.security.core.Authentication;
import org.springframework.stereotype.Component;

import java.util.Date;

@Component
public class JwtUtils {
	private static final Logger logger = LoggerFactory.getLogger(JwtUtils.class);

	@Value("${shop.app.jwtSecret}")
	private String jwtSecret;

	@Value("${shop.app.jwtExpirationMs}")
	private int jwtExpirationMs;

	public String generateJwtToken(Authentication authentication) {

		UserDetailsImpl userPrincipal = (UserDetailsImpl)
authentication.getPrincipal();

		return Jwts.builder()
				.setSubject((userPrincipal.getUsername()))
				.setIssuedAt(new Date())
				.setExpiration(new Date((new Date()).getTime() +
jwtExpirationMs))
				.signWith(SignatureAlgorithm.HS512, jwtSecret)
				.compact();
	}

	public String getUserNameFromJwtToken(String token) {
		return
Jwts.parser().setSigningKey(jwtSecret).parseClaimsJws(token).getBody().getSubject
();
	}
```

```
    public boolean validateJwtToken(String authToken) {
        try {

    Jwts.parser().setSigningKey(jwtSecret).parseClaimsJws(authToken);
            return true;
        } catch (SignatureException e) {
            logger.error("Invalid JWT signature: {}", e.getMessage());
        } catch (MalformedJwtException e) {
            logger.error("Invalid JWT token: {}", e.getMessage());
        } catch (ExpiredJwtException e) {
            logger.error("JWT token is expired: {}", e.getMessage());
        } catch (UnsupportedJwtException e) {
            logger.error("JWT token is unsupported: {}", e.getMessage());
        } catch (IllegalArgumentException e) {
            logger.error("JWT claims string is empty: {}", e.getMessage());
        }

        return false;
    }
}
```

Додаток В

Створення front-end та обробки даних

```
<template>
  <div class="login-container">
    <div class="    login-page " >

      <img
         id="profile-img"
         src="//ssl.gstatic.com/accounts/ui/avatar_2x.png"
         class="profile-img-card"
      />
      <form name="form" @submit.prevent="handleLogin">
        <div class=" login-pad">
          <input
             type="text"
             class="form-control "
             name="username"
             v-model="user.username"
             v-validate="'required'"
          />
          <div
             class="alert alert-danger"
             role="alert"
             v-if="errors.has('username')"
          >{{ $ml.get('msg.userNamedErr') }}
          </div>
        </div>
        <div class=" login-pad">
          <input
             type="password"
             class="form-control"
             :name="$ml.get('word.password')"
             v-model="user.password"
             v-validate="'required'"
          />
          <div
             class="alert alert-danger"
             role="alert"
             v-if="errors.has('password')"
```

Продовження додатку В

```
          >{{ $ml.get('msg.passwordErr') }}
          </div>

        </div>
        <div class=" login-pad">
          <button class="btn btn-primary btn-block" :disabled="loading">
            <span>{{ $ml.get('word.loginOnButton') }}</span>
          </button>
        </div>

        <!--        <div class="alert alert-danger" role="alert" v-if="message">{{
$ml.get('msg.authErr') }}</div>-->

<!--        <el-button @click="toRegistration()" type="text">{{
$ml.get('word.registration') }}</el-button>-->

      </form>

    </div>
  </div>
</template>

<script>
import User from "../../models/user";

export default {
  name: "login",
  computed: {
    loggedIn() {
      return this.$store.state.auth.status.loggedIn;
    }
  },
  data() {
    return {
      user: new User("", ""),
      loading: false,
      message: null
    };
  },
```

Продовження додатку В

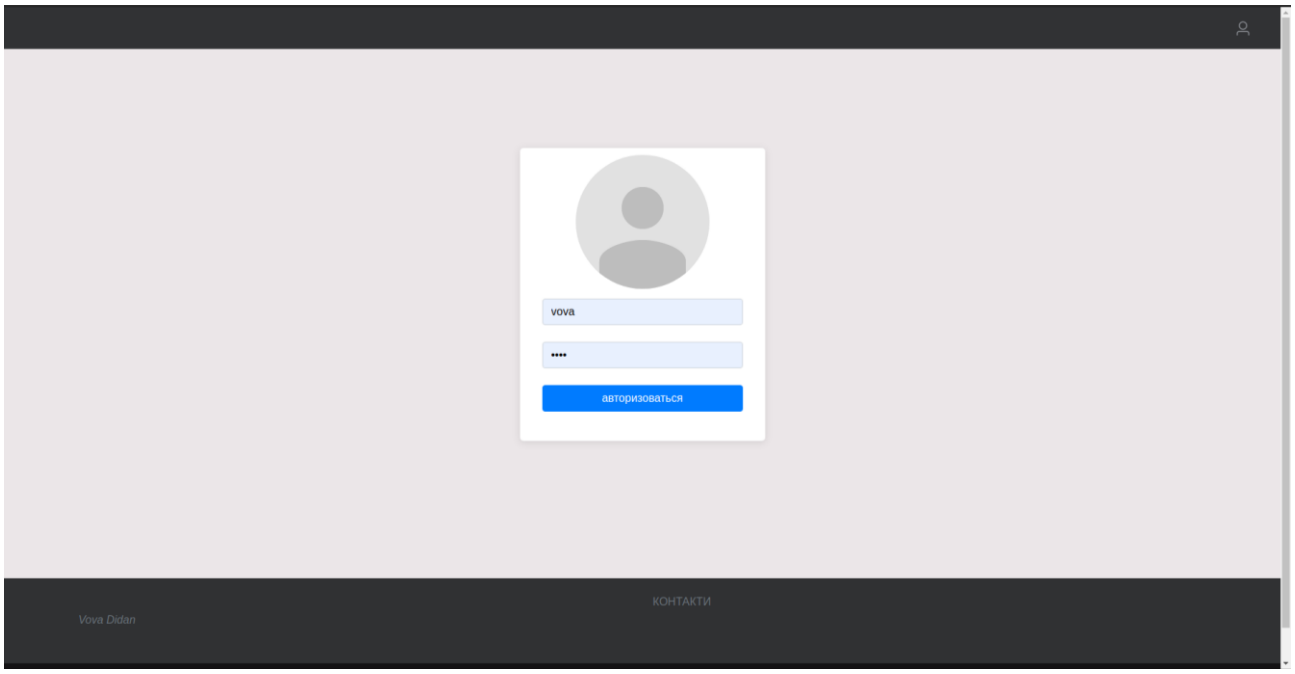
```
  mounted() {
    document.body.oncontextmenu = function () {
      return true;
    };
    if (this.loggedIn) {
      this.$router.push("/#/");
    }
  },
  methods: {

    handleLogin() {
      this.loading = true;
      this.$validator.validateAll();

      if (this.errors.any()) {
        this.loading = false;
        return;
      }

      if (this.user.username && this.user.password) {
        this.$store.dispatch("auth/login", this.user).then(
            () => {
              this.$router.push("/hello");
            },
            error => {
              this.loading = false;
              this.message = error;
              this.$message({
                showClose: true,
                type: 'error',
                message: this.$ml.get('msg.authErr') + ': ' + error.message
              })
            }
        );
      }
    }
  }
};
</script>
```

Продовження додатку В

```
<style>
.login-page {
  border-radius: 5px;
  box-shadow: 0 2px 12px 0 rgba(0, 0, 0, 0.1);
  max-width: 25rem;
  width: 22rem;
  min-width: 18rem;
  height: 420px;
background: white;
  position: relative;
  top: 15vh;
  text-align: center;
}

.login-container{
  background: #ebe6e8;

  height: 80vh;
  display: flex;
  flex-direction: column;
  justify-content: flex-start;
  align-items: center;
}

.login-pad {
  padding: 1.5rem 2rem 0rem;
}

.profile-img-card {

  position: relative;
  top:10px;
  border-radius: 100px;
}
</style>
```

Додаток Г

Вигляд сторінки авторизації



Додаток Ґ

Результат авторизації