МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 «Кібербезпека»

на тему: **ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ**

Студент групи СЗД-42 Корнієнко Андрій Юрійович _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Гребенніков Асаді Болдхоягович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н., доц. Г.В. Шуклін

«_____»_____ 2022р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Корнієнко Андрію Юрійовичу

1. Тема роботи: Захист інформаційних ресурсів автоматизованих систем управління технологічним процесом

Затверджена наказом по університеті від «16» лютого 2022 р. № 22

2. Термін здачі студентом оформленої роботи «____» _____ 2022 р.

3. Об'єкт дослідження: є процеси захисту інформаційних ресурсів автоматизованих систем обмеженого доступу.

4. Предмет дослідження: є методи і засоби захисту інформаційних ресурсів автоматизованих систем обмеженого доступу.

5. Мета роботи: створення комплексної системи захисту автоматизованих систем управління технологічним процесом з застосуванням сучасних програмних засобів.

6. Перелік питань, які мають бути розроблені:

1. Аналіз загроз інформації в автоматизованих системах обмеженого доступу.

2. Аналіз сучасних програмних засобів, які використовуються для автоматизації технологічних процесів.

3. Комплексна система захисту інформаційних ресурсів автоматизованих систем технологічного процесу.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____2022 р.

Науковий керівник _____ Шуклін Г.В.

Завдання прийняв до виконання _____ Корнієнко А.Ю.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз загроз інформації в автоматизованих системах обмеженого доступу		
2	Аналіз сучасних програмних засобів, які використовуються для автоматизації технологічних процесів		
3	Комплексна система захисту інформаційних ресурсів автоматизованих систем технологічного процесу		
4	Реферат, вступ, висновки		
5	Підготовка презентації до захисту		

Студент _____ Корнієнко А.Ю.

(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи _____ Шуклін Г.В.

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 88 сторінки, 8 малюнків, 8 таблиць, 25 джерел.

Об'єкт дослідження – Процеси захисту інформаційних ресурсів автоматизованих систем обмеженого доступу.

Предмет дослідження – Методи і засоби захисту інформаційних ресурсів автоматизованих систем обмеженого доступу.

Мета роботи - Створення комплексної системи захисту автоматизованих систем управління технологічним процесом з застосуванням сучасних програмних засобів.

Методи дослідження – теорія електрозв'язку, теорія інформації, системний аналіз.

В роботі проведено дослідження вимог чинного законодавства України щодо захисту інформації в інформаційно-телекомунікаційній системі. В рамках роботи проведено обстеження середовищ функціонування інформаційно-телекомунікаційної системи, розроблені моделі загроз інформаційній безпеки та моделі порушника, політика інформаційної безпеки і технічне завдання. Проаналізовано сучасні програмні засоби, та обрано конкретні для захисту інформації в АС класу 1.

Галузь використання – інформаційна безпека.

ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, АНТИВІРУС ПРОФІЛЬ ЗАХИЩЕНОСТІ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АКТИВНІ МЕТОДИ ЗАХИСТУ.

ANNOTATION

The text part of bachelor work: 82 pages, 9 figures, 8 tables, 25 sources.

Object of research - Protection of information in information and telecommunication systems.

Subject of research - Modern software tools.

The purpose of the work is to create a comprehensive information security system in the automated system of class 1 with the use of modern software tools.

Methods of research - telecommunication theory, information theory, system analysis.

In this work the study of the requirements of the current legislation of Ukraine concerning the protection of information in the information and telecommunication system has been conducted. Within the framework of the work, a survey of the functioning of the information and telecommunication system was carried out, models of information security threats and violator model, information security policy and a technical task were developed. The modern software tools have been analyzed, and concrete ones have been selected for the protection of information in the Class 1 AU.

The field of use is information security.

INFORMATION WITH RESTRICTED ACCESS, COMPLEX OF PROTECTION, ANTI-VIRUS PROFILE SECURITY, OBJECT OF INFORMATIONAL ACTIVITY, ACTIVE PROTECTION METHODS.

ЗМІСТ

ВСТУП

На даний час в провідних країнах світу склалася досить чітко окреслена система концептуальних поглядів на проблеми забезпечення інформаційної безпеки. Проте, як свідчить сьогодення, злочинні дії пов’язані з інформацією як у приватному так і не тільки не зменшуються, але і мають досить стійку тенденцію до зростання. Розуміючи це, більшість керівників підприємств і організацій вживають заходів щодо захисту важливої для них інформації.

Для вирішення завдань захисту інформації створюється комплексна система захисту інформації. Під інформаційною безпекою будемо розуміти стан захищеності інформаційного середовища підприємства, який забезпечує його функціонування і розвиток в інтересах організації. Управляння інформаційною безпекою – це сукупність заходів, призначених для досягнення і підтримання стану захищеності.

Мета роботи – Створення комплексної системи захисту інформації в автоматизованій системі класу 1 з застосуванням сучасних програмних засобів.

Об’єкт дослідження – Захист інформації в інформаційно-телекомунікаційних системах.

Предмет дослідження – Сучасні програмні засоби..

У даній роботі розглядається методика створення комплексної системи захисту інформації в АС класу 1 з застосуванням сучасних програмних засобів.

Галузь застосування – інформаційна безпека.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОІД - об'єкт інформаційної діяльності

ОС - обчислювальна система

АС - автоматизована система

КС - комп’ютерна система

КЗЗ - комплекс засобів захисту

ІзОД - інформація з обмеженим доступом

КСЗІ - комплексна система захисту інформації

ІТС – інформаційно-телекомунікаційна система

ТЗІ - технічний захист інформації

ОТЗС - основні технічні засоби і системи

ТЗПІ - технічний засіб перетворення інформації

ДТЗС - допоміжні технічні засоби системи

ПЕМВ - побічні електромагнітні випромінювання

ПЕВІН - побічні електромагнітні випромінювання і наведення

1 ІНФОРМАЦІЙНА БЕЗПЕКА В АВТОМАТИЗОВАНИХ СИСТЕМАХ КЛАСУ 1

1.1. Вимоги до її захисту

Закон України "Про інформацію" класифікує всю інформацію за режимом правового доступу, тобто відповідно до передбаченого правовими нормами порядку її отримання, використання, зберігання наступним чином [1]:

- відкрита що належіть особі;
- відкрита що належіть державі;
- конфіденційна, що належіть особі;
- конфіденційна, що належіть державі;
- службова;
- та що становить державну таємницю.

Інформаційна безпека – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації (НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу).

Для характеристики основних властивостей інформації використовується модель CIA (конфіденційність (англ. Confidentiality, privacy), цілісність (англ. Integrity), доступність (англ. Availability), але враховуючи НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу з’являються й інші властивості:

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Таємна інформація(секретна інформація) – вид інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом, державною таємницею і підлягають охороні державою. До секретної(особливої важливості – ОВ, цілком таємної – ЦТ, таємної – Т) відноситься інформація, що містить відомості, які становлять державну або іншу передбачену законом таємницю, розголошення якої завдає шкоди суспільству (державі) [7].

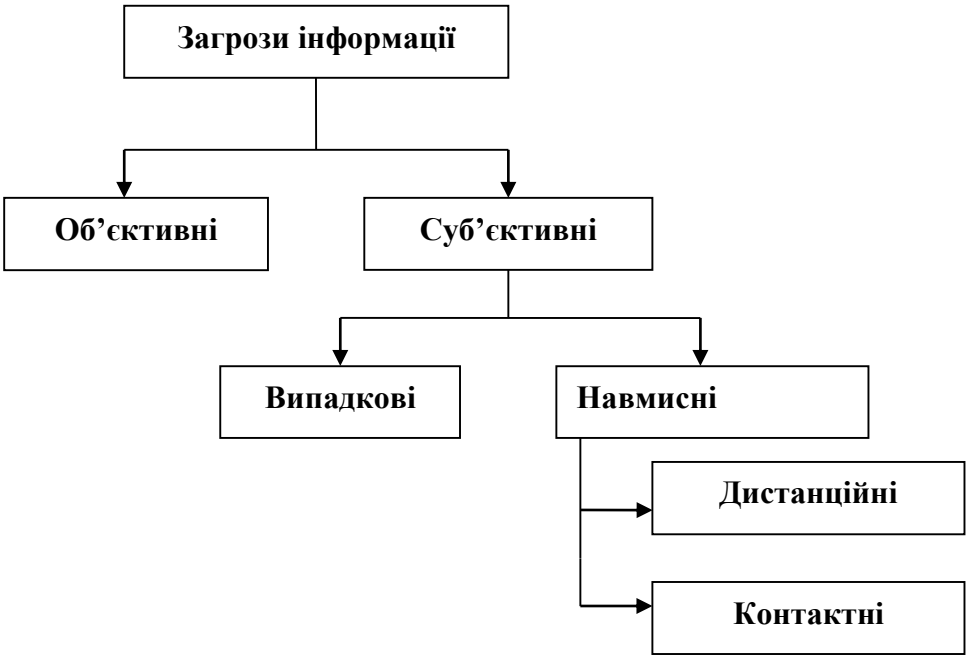
У відповідності до вимог Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення. [2]

1.2. Загрози інформації в автоматизованих системах класу 1

Для забезпечення конфіденційності, цілісності та доступності інформації, а також керованості системою існує необхідність захисту інформації не тільки від витоку технічними каналами та несанкціонованого доступу, а також захисту самої системи (об’єкта), в якій (на якому) циркулює інформації від втручання в процес її обробки, порушення працездатності системи.

Найбільш частішими та небезпечними є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. Іноді такі помилки є загрозами (невірно введені дані, помилка в програмі, котра викликає колапс системи), іноді вони створюють ситуації, якими не лише можуть скористатися зловмисники, а які самі по собі становлять безпосередню небезпеку об'єкта. Яскравим прикладом є уведення невірної інформації в комп'ютер швейцарським оператором на землі, внаслідок чого у небі зіткнулося два літаки, в одному з яких летіли діти з Росії. Наслідки були трагічними як для пасажирів літака, так і для оператора, якого через деякий час після катастрофи було навмисно вбито.

У цілому ж, за результатами проведених фахівцями з інформаційної безпеки досліджень, понад 65 % шкоди, яка завдається інформаційним ресурсам, є наслідком ненавмисних помилок. Пожежі та землетруси, тобто загрози природного характеру, трапляються набагато рідше. В загальному випадку загрози можна розподілити наступним чином (мал. 1.1):



Мал. 1.1. Загальна класифікація загроз інформації

За мотивами походження суб’єктивні загрози поділяються на випадкові і навмисні. Випадкові загрози викликаються помилками проектування автоматизованої системи і системи захисту інформації, помилками в програмному забезпеченні, збоями та відмовами апаратури і систем забезпечення, помилками персоналу тощо. Навмисні загрози обумовлені цілеспрямованими діями людей (порушників);

за місцем розміщення джерела загроз щодо автоматизованої системи навмисні загрози поділяються дистанційні та контактні. До дистанційним відносяться загрози, джерело яких знаходиться за межами контрольованої території. Контактні загрози здійснюються в межах контрольованої зони, як правило, при проникненні в приміщення, де розташовані засоби обробки і зберігання інформації;

за типом основного засобу, який використовується для реалізації загрози, всі джерела загроз поділяються на групи, де такими є: людина, апаратура, програма, фізичне середовище.

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) за результатами впливу на інформацію і систему її обробки загрози поділяються на чотири класи:

порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);

порушення цілісності (повне або часткове знищення, викривлення, модифікація, нав'язування неправдивої інформації);

порушення доступності інформації (втрата часткова або повна працездатності системи, блокування доступу до інформації);

втрата спостережливості або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів і процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

Потенційні загрози інформації, яка обробляється в автоматизованій системі класу 1 наступні:

- відключення забезпечення функціонування системи;

- дезорганізації функціонування системи;

- впровадження агентів у число працівників системи;

- перехоплення ПЕМВН;

- розкрадання матеріальних носіїв;

- незаконне одержання реквізитів розмежування доступу;

- ненавмисні дії, що призводять до часткового або повного відмовлення системи

- неправомірне включення;

- розробка програм, що представляють небезпеку для працездатності;

- видалення помилкових даних.

На завершення розгляду технічних каналів витоку інформації слід особливо зупиниться на такому актуальному питанні, як канали витоку інформації, що утворюються при експлуатації персональних електронно-обчислювальних машин (ПЕОМ), або персональних комп'ютерів (ПК).

Дійсно, з точки зору захисту інформації ці технічні пристрої є прекрасним прикладом для вивчення практично всіх каналів витоку інформації - починаючи від радіоканалу і закінчуючи матеріально-речовим. З огляду на роль, яку відіграють ПЕОМ в сучасному суспільстві взагалі, а також тенденцію до повсюдного використання ПЕОМ для обробки інформації з обмеженим доступом зокрема, абсолютно необхідно детальніше розглянути принципи утворення каналів витоку інформації при експлуатації ПЕОМ.

Як відомо, сучасні ПЕОМ можуть працювати як незалежно один від одного, так і взаємодіючі з іншими ЕОМ по комп'ютерних мережах, причому останні можуть бути не тільки локальними, а й глобальними.

З урахуванням цього фактору, повний перелік тих ділянок, в яких можуть знаходитися підлягають захисту дані, може мати наступний вигляд:

безпосередньо в оперативній або постійної пам'яті ПЕОМ;

на знімних магнітних, магнітооптичних, лазерних та інших носіях;

на зовнішніх пристроях зберігання інформації колективного доступу (RAID-масиви, файлові сервери і);

на екранах пристроїв відображення (дисплеї, монітори, консолі);

в пам'яті пристроїв введення / виведення (принтери, графічні, сканери);

в пам'яті керуючих пристроїв і лініях зв'язку, що утворюють канали сполучення комп'ютерних мереж.

Канали витоку інформації утворюються як при роботі ЕОМ, так і в режимі очікування. Джерелами таких каналів є:

електромагнітні поля;

наводяться струми і напруги в провідних системах (живлення, заземлення та з'єднування);

випромінювання оброблюваної інформації на частотах паразитної генерації елементів і пристроїв технічних засобів (ТЗ) ЕОМ;

випромінювання оброблюваної інформації на частотах контрольно-вимірювальної апаратури (КВА).

Крім цих каналів, обумовлених природою процесів, що протікають в ПЕОМ та їх технічними особливостями, в що поставляються на ринок ПЕОМ можуть навмисне створюватися додаткові канали витоку інформації. Для освіти таких каналів може використовуватися: розміщення в ПЕОМ закладок на мову або оброблювану інформацію (замасковані під будь-які електронні блоки):

установка в ПЕОМ радіомаячків;

умисне застосування таких конструктивно-схемних рішень, які призводять до збільшення електромагнітних випромінювань в певній частині спектра;

установка закладок, що забезпечують знищення ПЕОМ ззовні (схемні рішення);

установка елементної бази, що виходить з ладу.

Крім того, класифікацію можливих каналів витоку інформації в першому наближенні можна провести на підставі принципів, відповідно до яких обробляється інформація, що отримується з можливого каналу витоку. Передбачається три типи обробки: людиною, апаратурою, програмою. Відповідно

до кожного типу обробки всілякі канали витоку також розбиваються на три групи. Стосовно до ПЕОМ групи каналів, в яких основним видом обробки є обробка людиною, складають наступні можливі канали витоку:

розкрадання матеріальних носіїв інформації (магнітних дисків, стрічок, карт);

читання інформації з екрану сторонньою особою;

читання інформації з залишених без нагляду паперових роздруківок.

У групі каналів, в яких основним видом обробки є обробка апаратурою, можна виділити наступні можливі канали витоку:

підключення до ПЕОМ спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань технічних засобів ПЕОМ.

У групі каналів, в яких основним видом обробки є програмна обробка, можна виділити наступні можливі канали витоку:

несанкціонований доступ програми до інформації;

розшифровка програмою зашифрованої інформації;

копіювання програмою інформації з носіїв;

блокування або відключення програмних засобів захисту.

При цьому технічному контролю повинні піддаватися наступні потенційні канали витоку інформації:

побічні електромагнітні випромінювання в діапазоні частот від 10 Гц до 100 МГц;

наведення сигналів в ланцюгах електроживлення, заземлення і в лініях зв'язку;

небезпечні сигнали, що утворюються за рахунок електроакустичних перетворень, які можуть відбуватися в спеціальній апаратурі контролю інформації. Ці сигнали повинні контролюватися в діапазоні частот від 300 Гц до 3,4 кГц;

канали витоку інформації, що утворюються в результаті впливу високочастотних електромагнітних полів на різні дроти, які знаходяться в

приміщенні і можуть, таким чином, стати прийомною антеною. В цьому випадку перевірка проводиться в діапазоні частот від 20 кГц до 100 МГц.

Схеми адаптера формують сигнали, що визначає інформацію, яка відображається на екрані. Для цього в усіх відеосистемах є відеобуфер. Він являє собою область оперативної пам'яті, яка призначена тільки для зберігання тексту або графічної інформації, виведеної на екран. Основна функція відеосистеми полягає в перетворенні даних з відеобуфера в керуючі сигнали дисплея, за допомогою яких на його екрані формується зображення. Ці сигнали і намагаються перехопити. Розглянемо докладніше можливості витоку інформації, що обробляється на ПЕОМ, через побічні електромагнітні випромінювання (ПЕМВ).

1.3. Захист інформації в автоматизованих системах класу 1

Комплексна система захисту інформації (КСЗІ) є підходом до організації системи захисту інформації, при якому вона інтегруються у всі компоненти інформаційної системи, що захищається, в якій обробляється інформація, що захищається, і надає цілісний і достатній набір засобів захисту від актуальних загроз ІБ, реалізуючи проактивну, активну і реактивну моделі захисту інформації та використовуючи різні напрями забезпечення безпеки.

Система призначена захисту інформації, оброблюваної на автономному комп'ютері, чи комп'ютерах у складі корпоративної мережі. КСЗІ служить для ефективної протидії, як відомим, так і потенційно можливим атакам на ресурси, що захищаються, що забезпечується усуненням архітектурних недоліків захисту сучасних ОС. КСЗІ також може використовуватися для ефективної протидії вірусним атакам та шпигунським програмам. Необхідність побудови КСЗІ

Необхідність побудови КСЗІ визначається вимогами нормативних документів чи бажанням власника інформаційних ресурсів.

Комплексний захист інформації включає розробку, виробництво та встановлення технічних засобів захисту, а також регулярне проведення перевірок використовуваного інформаційного обладнання.

Об'єктами захисту КСЗІ є інформація, у будь-якому її вигляді та формі подання. Матеріальними носіями є сигнали. За своєю фізичною природою інформаційні сигнали можна розділити такі види: електричні, електромагнітні, акустичні, і навіть їх комбінації. Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видах коливань, причому інформація, яка підлягає захисту, міститься в їх параметрах, що змінюються. Тільки комплексний підхід до побудови системи захисту дозволяє організувати цілісну систему захисту від загроз.

Організаційний захист - це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояв внутрішніх та зовнішніх загроз. Головними цілями організаційного захисту інформації є забезпечення сталого функціонування підприємства та запобігання загрозам його безпеці, захист законних інтересів організації від протиправних посягань, недопущення розкрадання фінансових та матеріально-технічних засобів, знищення майна та цінностей, розголошення, витоку та несанкціонованого доступу до службової інформації, порушення технічних засобів забезпечення виробничої діяльності, включаючи засоби інформатизації. Організаційний захист забезпечує:

організацію охорони, режиму, роботу з кадрами, документами;

використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх та зовнішніх загроз підприємницької діяльності.

Засоби криптографічного захисту інформації (СКЗІ) — спеціальні пристрої, служби або програми, що забезпечують шифрування (кодування) та розшифрування (розкодування) інформації з метою її захисту від несанкціонованої обробки, доступу та зберігання при обміні нею каналами зв'язку, а також відповідальні за генерацію електронної підписи (ЕП).

При шифруванні кожен символ документа, що передається каналом зв'язку, підлягає кодуванню, а сама інформація, яку необхідно захистити, поділяється на окремі блоки, кожен з яких замінюється кодом: буквеним, цифровим або комбінованим. Також широко використовуються такі методи шифрування, як перестановка, заміна, аналітичне перетворення та гамування.

Основа роботи СКЗІ у тому, що створений користувачем інформаційний документ з'єднується з файлом електронного підпису, навіщо застосовується власний закритий ключ цифрового підпису. Отримувач розшифровує отриманий файл за допомогою СКЗІ та власного ключа цифрового підпису. Далі одержувач переконується в тому, що отриманий файл не вносилися правки і що електронний підпис ціла..

Інженерний захист інформації — попередження руйнування носія інформації внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація). Технічний захист інформації призначений для вирішення наступних задач:

- захист інформації від несанкціонованого доступу;

- захист інформації від витоку технічними каналами.

Для забезпечення ТЗІ створюється комплекс технічного захисту інформації, який є складовою КСЗІ.

Під несанкціонованим доступом до інформації (НСД) розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Несанкціонований доступ може здійснюватися як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу КС розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

До основних способів НСД відносяться:

- безпосереднє звертання до об'єктів з метою одержання певного виду доступу;

- створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;

- модифікація засобів захисту, що дозволяє здійснити НСД;

- впровадження в КС програмних або апаратних механізмів, що порушують структуру і функції КС і дозволяють здійснити НСД.

Засіб технічного захисту інформації від НСД – це програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну програмну та/або конструкторську документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз НСД для інформації в КС, або використовується для контролю ефективності захисту інформації від НСД в таких системах.

Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок, акустичні канали, оптичні канали та інші.

Захист від НСД може здійснюватися в різних *складових* інформаційної системи:

- прикладне та системне ПЗ.

- апаратна частина серверів та робочих станцій.

- комунікаційне обладнання та канали зв'язку.

ТЗІ від НСД на прикладному і програмному рівні

Для захисту інформації на рівні прикладного та системного ПЗ використовуються:

- системи розмежування доступу до інформації;

- системи ідентифікації та автентифікації;

- системи аудиту та моніторингу;

- системи антивірусного захисту.

ТЗІ від НСД на апаратному рівні

Для захисту інформації на рівні апаратного забезпечення використовуються:

- апаратні ключі

- системи сигналізації

- засоби блокування пристроїв та інтерфейсів вводу-виводу інформації.

ТЗІ на мережевому рівні

В комунікаційних системах використовуються такі засоби мережевого захисту інформації:

між мережеві екрани — для блокування атак з зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway та Alteon Switched Firewall від компаніїNortel Networks). Вони керують проходженням мереженого трафіку відповідно до правил захисту. Як правило, між мережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі;

системи виявлення утручань — для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert та NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі;

засоби створення віртуальних приватних мереж — для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування;

засоби аналізу захищеності — для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації (Symantec Enterprise Security Manager, Symantec Net Recon). Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Захист інформації від її витоку технічними каналами зв'язку забезпечується такими засобами та заходами:

використанням екранованого кабелю та прокладка проводів та кабелів в екранованих конструкціях;

встановленням на лініях зв'язку високочастотних фільтрів;

побудовою екранованих приміщень «капсул»;

використанням екранованого обладнання;

встановленням активних систем зашумлення;

створенням контрольованої зони.

Для забезпечення безпеки інформації в мережах проводяться різні заходи, що об'єднуються поняттям «система захисту інформації». Система захисту інформації – це сукупність заходів, програмно-технічних засобів, правових та морально-етичних норм, спрямованих на протидію загрозам порушників з метою зведення до мінімуму можливих збитків користувачам і власникам системи.

До технічних заходів можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок, установку устаткування виявлення і гасіння пожежі, устаткування виявлення води, прийняття конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів, установку резервних систем електроживлення, оснащення приміщень замками, установку сигналізації і багато чого іншого.

До організаційних заходів можна віднести охорону серверів, ретельний підбір персоналу, виключення випадків ведення особливо важливих робіт лише однією людиною, наявність плану відновлення працездатності сервера після виходу його з ладу, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво).

Несанкціонований доступ до інформації може відбуватися під час профілактики або ремонту комп'ютерів за рахунок прочитання залишкової інформації на носіях, незважаючи на її видалення користувачем звичайними методами. Інший спосіб - прочитання інформації з носія під час його транспортування без охорони всередині об'єкта або регіону.

Сучасні комп'ютерні засоби побудовані на інтегральних схемах. При роботі таких схем відбуваються високочастотні зміни рівнів напруги і струмів, що призводить до виникнення в ланцюгах харчування, в ефірі, в близько розташованій

апаратурі і т.д. електромагнітних полів і наведень, які за допомогою спеціальних засобів (умовно назвемо їх "шпигунськими") можна трансформувати в оброблювану інформацію. Зі зменшенням відстані між приймачем порушника та апаратними засобами ймовірність такого роду знімання і розшифровки інформації збільшується.

Несанкціоноване ознайомлення з інформацією можливо також шляхом безпосереднього підключення порушником «шпигунських» коштів до каналів зв'язку і мережевим апаратних засобів.

Традиційними методами захисту інформації від несанкціонованого доступу є ідентифікація та автентифікація, захист паролями.

Ідентифікація та автентифікація. У комп'ютерних системах зосереджується інформація, право на користування якою належить певним особам або групам осіб, що діють у порядку особистої ініціативи або відповідно до посадових обов'язків. Щоб забезпечити безпеку інформаційних ресурсів, усунути можливість несанкціонованого доступу, посилити контроль санкціонованого доступу до конфіденційної або до підлягає засекречування інформації, впроваджуються різні системи розпізнавання, встановлення дійсності об'єкта (суб'єкта) і розмежування доступу. В основі побудови таких систем знаходиться принцип допуску та виконання тільки таких звернень до інформації, в яких присутні відповідні ознаки дозволених повноважень.

Ключовими поняттями в цій системі є ідентифікація та автентифікація. Ідентифікація – це присвоєння будь-якого об'єкта чи суб'єкту унікального імені або образу. Автентифікація– це встановлення автентичності, тобто перевірка, чи є об'єкт (суб'єкт) дійсно тим, за кого він себе видає.

Кінцева мета процедур ідентифікації і автентифікації об'єкта (суб'єкта) – допуск його до інформації обмеженого користування у разі позитивної перевірки або відмова в допуску у випадку негативного результату перевірки.

Об'єктами ідентифікації і автентифікації можуть бути: люди (користувачі, оператори та ін); технічні засоби (монітори, робочі станції, абонентські пункти);

документи (ручні, друку та ін); магнітні носії інформації; інформація на екрані монітора та ін.

Встановлення дійсності об'єкта може здійснюватися апаратним пристроєм, програмою, людиною і т.д.

Захист паролями. Пароль - це сукупність символів, що визначає об'єкт (суб'єкта). При виборі пароля виникають питання про його розмір, стійкості до несанкціонованого добору, способам його застосування. Природно, чим більше довжина пароля, тим більшу безпеку буде забезпечувати система, бо потрібні великі зусилля для його відгадування. При цьому вибір довжини пароля в значній мірі визначається розвитком технічних засобів, їх елементної базою і швидкодією.

У разі застосування пароля необхідно періодично замінювати його на новий, щоб знизити ймовірність його перехоплення шляхом прямого розкрадання носія, зняття її копії та навіть фізичного примусу людини. Пароль вводиться користувачем на початку взаємодії з комп'ютерною системою, що іноді і в кінці сеансу (в особливо відповідальних випадках пароль нормального виходу може відрізнятися від вхідного). Для правомочності користувача може передбачатися введення пароля через певні проміжки часу.

Пароль може використовуватися для ідентифікації і встановлення автентичності терміналу, з якого входить в систему користувач, а також для зворотного встановлення автентичності комп'ютера по відношенню до користувача.

Для ідентифікації користувачів можуть застосовуватися складні у плані технічної реалізації системи, що забезпечують встановлення автентичності користувача на основі аналізу його індивідуальних параметрів: відбитків пальців, малюнка ліній руки, райдужної оболонки очей, тембру голосу і ін.

Широке поширення знайшли фізичні методи ідентифікації з використанням носіїв кодів паролів. Такими носіями є пропуску в контрольно-пропускних системах; пластикові картки з ім'ям власника, його кодом, підписом; пластикові картки з магнітною смугою; пластикові карти з вбудованою мікросхемою (smart-card); карти оптичної пам'яті та ін.

Засоби захисту інформації з методів реалізації можна розділити на три групи: програмні; програмно-апаратні; апаратні.

Програмними засобами захисту інформації називаються спеціально розроблені програми, які реалізують функції безпеки обчислювальної системи, здійснюють функцію обмеження доступу користувачів по паролях, ключам, багаторівневому доступу і т.д. Ці програми можуть бути реалізовані практично в будь-якій операційній системі, зручною для користувача. Як правило, ці програмні засоби забезпечують досить високу ступінь захисту системи і мають помірні ціни. При підключенні такої системи в глобальну мережу ймовірність злому захисту збільшується. Отже, цей спосіб захисту прийнятний для локальних замкнених мереж, не мають зовнішній вихід.

Програмно-апаратними засобами називаються пристрої, реалізовані на універсальних або спеціалізованих мікропроцесорах, які не потребують модифікацій в схемотехниці при зміні алгоритму функціонування. Ці пристрої також адаптуються в будь-якій операційній системі, мають велику ступінь захисту. Вони обійдуться дещо дорожче (їх ціна залежить від типу операційної системи). При цьому даний тип пристроїв є самим гнучким інструментом, що дозволяє вносити зміни в конфігурацію на вимогу замовника. Програмно-апаратні засоби забезпечують високу ступінь захисту локальної мережі, підключеного до глобальної.

Апаратними засобами називаються пристрої, в яких функціональні вузли реалізуються на надвеликих інтегральних системах (НВІС) з незмінним алгоритмом функціонування. Цей тип пристроїв адаптується в будь-якій операційній системі, є найдорожчим в розробці, пред'являє високі технологічні вимоги при виробництві. У той же час ці пристрої володіють найвищим ступенем захисту, в них неможливо потрапити і внести конструктивні чи програмні зміни. Застосування апаратних засобів ускладнений через їх високу вартість і статичності алгоритму.

Програмно-апаратні засоби, поступаючись апаратним за швидкістю, дозволяють у той же час легко модифікувати алгоритм функціонування і не володіють недоліками програмних методів.

До окремої групи заходів щодо забезпечення збереження інформації та виявлення несанкціонованих запитів відносяться програми виявлення порушень в режимі реального часу.

Криптографічні засоби захисту інформації, найбільший інтерес сьогодні викликають наступні напрямки теоретичних і прикладних досліджень: створення та аналіз надійності криптографічних алгоритмів та протоколів; адаптація алгоритмів до різних апаратних і програмних платформ; використання існуючих технологій криптографії в нових прикладних системах; можливість використання технологій криптографії для захисту інтелектуальної власності.

Існуючі засоби захисту даних у телекомунікаційних мережах можна розділити на дві групи за принципом побудови ключової системи та системи автентифікації. До першої групи віднесемо кошти, які використовують для побудови ключової системи та системи автентифікації симетричні криптоалгоритми, до другої - асиметричні.

Проведемо порівняльний аналіз цих систем. Готове до передачі інформаційне повідомлення, спочатку відкрите і незахищене, зашифровується і тим самим перетворюється в шифрограму, тобто в закриті текст або графічне зображення документа. У такому вигляді повідомлення передається по каналу зв'язку, навіть і не захищеного. Санкціонований користувач після отримання повідомлення дешифрує його (тобто розкриває) за допомогою зворотного перетворення криптограми, внаслідок чого виходить вихідний, відкритий вид повідомлення, доступний для сприйняття санкціонованим користувачам.

Методу перетворення в криптографічного системі відповідає використання спеціального алгоритму. Дія такого алгоритму запускається унікальним числом (послідовністю біт), зазвичай званим шифрувальним ключем. Для більшості систем схема генератора ключа може являти собою набір інструкцій і команд який вузол апаратури, або комп'ютерну програму, або все це разом, але в будь-якому

випадку процес шифрування (дешифрування) реалізується тільки цим спеціальним ключем. Щоб обмін зашифрованими даними проходив успішно, як відправнику, так і одержувачу, необхідно знати правильну ключову установку і зберігати її в таємниці.

Стійкість будь-якої системи закритого зв'язку визначається ступенем секретності використовуваного в ній ключа. Тим не менш, цей ключ має бути відомий іншим користувачам мережі, щоб вони могли вільно обмінюватися зашифрованими повідомленнями. У цьому сенсі криптографічні системи також допомагають вирішити проблему автентифікації (встановлення достовірності) прийнятої інформації. Зломщик у разі перехоплення повідомлення буде мати справу тільки з зашифрованим текстом, а істинний одержувач, приймаючи повідомлення, закриті відомим йому і відправнику ключем, буде надійно захищена від можливої дезінформації.

Крім того, існує можливість шифрування інформації і більш простим способом - з використанням генератора псевдовипадкових чисел. Використання генератора псевдовипадкових чисел полягає в генерації гами шифру за допомогою генератора псевдовипадкових чисел при певному ключі та накладення отриманої гами на відкриті дані оборотним способом. Цей метод криптографічного захисту реалізується досить легко і забезпечує досить високу швидкість шифрування, однак недостатньо стійкий до дешифрування.

Для класичної криптографії характерне використання однієї секретної одиниці - ключа, який дозволяє відправнику зашифрувати повідомлення, а одержувачу розшифрувати його. У разі шифрування даних, що зберігаються на магнітних чи інших носіях інформації, ключ дозволяє зашифрувати інформацію під час запису на носій і розшифрувати при читанні з нього.

З викладеного випливає, що надійна криптографічна система повинна задовольняти ряду певних вимог:

процедури зашифровування та розшифрування повинні бути «прозорі» для користувача;

дешифрування закритої інформації має бути максимально ускладнено;

зміст переданої інформації не повинно позначатися на ефективності криптографічного алгоритму.

Найбільш перспективними системами криптографічного захисту даних сьогодні вважаються асиметричні криптосистеми, звані також системами з відкритим ключем. Їх суть полягає в тому, що ключ, використовуваний для зашифровування, відмінний від ключа розшифрування. При цьому ключ зашифровування не секрет і може бути відомий всім користувачам системи. Однак розшифрування за допомогою відомого ключа зашифровування неможливо. Для розшифрування використовується спеціальний, секретний ключ. Знання відкритого ключа не дозволяє визначити ключ секретний. Таким чином, розшифрувати повідомлення може тільки його одержувач, що володіє цим секретним ключем.

Фахівці вважають, що системи з відкритим ключем більше підходять для шифрування переданих даних, ніж для захисту даних, що зберігаються на носіях інформації.

Криптографія надає можливість забезпечити безпеку інформації в INTERNET і зараз активно ведуться роботи з впровадження необхідних криптографічних механізмів в цю мережу. Не відмова від прогресу в інформатизації, а використання сучасних досягнень криптографії - ось стратегічно правильне рішення. Можливість широкого використання глобальних інформаційних мереж та криптографії є досягненням і ознакою демократичного суспільства.

Висновок по розділу: завдяки аналізу Законів України визначаємо види та вимоги до захисту ІЗоД, окреслюємо види загроз на об’єктах інформаційної діяльності, та досліджуємо способи та засоби захисту інформації такі як: захист від НСД та захист витоку технічними каналами шляхом реалізації КТЗІ.

2 ПОБУДОВА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ КЛАСУ 1

2.1. Обстеження середовищ функціонування АС - 1

Обстеження обчислювальної системи

До складу обчислювальної системи АС-1 входять такі компоненти:

ПЕОМ у комплекті з клавіатурою, маніпулятором типу «миша», монітором, шнурами електроживлення;

ПК Office AMD Plus Блок системный "FORWARD-office" AMD Sempron X4 3850 (1.3 ГГц) / ОЗУ 4 Gb / НЖМД 320 Gb / Radeon R3 int / lan / 400W / ОС XP.

Обстеження фізичного середовища

Контрольована зона (КЗ) АС-1 визначена Планом КЗ будівлі 4-б по вул. Андрющенка. Інв. № 195 від 30.01.2012.

АС-1 розташована за адресою: (поштовий код), м. Київ, 01132.

Більш детальний опис фізичного середовища наведений у Акті обстеження.

Обстеження середовища користувачів

За рівнем повноважень, щодо характеру та змісту робіт, які виконуються в процесі функціонування АС-1 , суб‘єкти доступу до АС-1 поділяються на таких, що мають доступ до інформаційних об’єктів системи та таких що не мають.

Суб’єкти доступу, що мають можливість ознайомлення із інформаційними об’єктами системи, що містять відомості, які відносяться інформації до службової інформації, підрозділяються на такі категорії:

користувачі, які мають певні повноваження щодо оброблення ІзОД в АС- 1 (працівники, які допущені до роботи з ІзОД в АС-1);

користувачі, які мають повноваження щодо встановлення та керування КЗЗ, технічний персонал, який забезпечує працездатність АС-1, встановлення та налаштування системного, прикладного та сервісного програмного забезпечення (адміністратор безпеки, системний адміністратор);

службовий персонал, який забезпечує порядок у робочих приміщеннях, контролює дотримання вимог санітарних, протипожежних та інших норм на території приміщення, в якому функціонує АС-1.

Користувач АС-1, відповідно до особливостей технології обробки інформації в АС-1, може отримувати доступ виключно до ІзОД, яка міститься в файлах та каталогах на зареєстрованому за цим користувачем носієві (за потреби) або збереженій у відповідних каталогах на жорсткому диску (див. «Інструкція користувача щодо роботи в АС»).

Адміністратор безпеки (системний адміністратор) з метою контролю коректності виконання функцій збереження даних ІзОД може отримувати доступ до файлів та каталогів, які містять відомості ІзОД, якщо вони були некоректно збережені в окремих об’єктах АС-ІІБ та не були видаленими штатними засобами очищення КЗЗ.

До категорій суб’єктів, які здійснюють обслуговування приміщення № 33, без необхідності доступу до ресурсів АС-1, відноситься технічний персонал, який забезпечує працездатність АС-1 (системний адміністратор).

Системний адміністратор виконує свої функціональні обов’язки згідно з «Інструкцією системного адміністратора АС», під контролем адміністратора безпеки, та діє в рамках організаційних обмежень, встановлених призначеною йому роллю.

До складу суб’єктів, які здійснюють обслуговування приміщення № 33, без необхідності доступу до ресурсів АС-1, відноситься технічний персонал, який забезпечує порядок у робочих приміщеннях, контролює дотримання вимог санітарних, охоронних, протипожежних та інших норм.

Типові режимні умови стосовно доступу суб’єктів до ресурсів АС-1 передбачають наступне:

доступ службового та технічного персоналу дозволяється лише за присутності адміністратора безпеки або відповідальної особи;

доступ користувачів до ІзОД дозволяється лише у разі необхідності та в рамках виконання покладених на них обов‘язків.

Доступ інших суб’єктів до програмно-апаратних засобів АС-1 (розробники ПЗ, КСЗІ, техніки із планового супроводження апаратного обладнання) дозволяється лише під наглядом адміністратора безпеки; попередньо адміністратором мають бути проведені всі необхідні заходи щодо перевірки відсутності в АС-1 інформаційних об’єктів, які містять ІзОД.

2.2. Розробка акту обстеження на об’єкті інформаційної діяльності

Для службового користування

(після заповнення)

Прим. № _1

ЗАТВЕРДЖЕНО

Ген. Дир.

Коваленко А.С.

_01__ _10_____2017_

АКТ

обстеження на об’єкті інформаційної діяльності

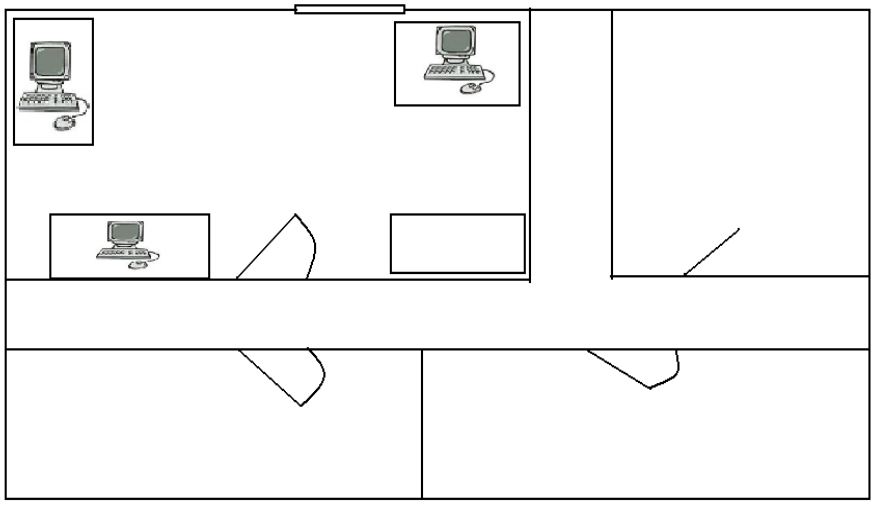
_____ТОВ «Радар» вул.. Ахматової 12_____

(назва, належність об'єкта інформаційної діяльності)

1. Обстеження на ОІД проведено 15 09 2018 р. комісією у складі: голова комісії Смірнов В.А., члени: Сорокін В.Д. Курков С.С., згідно із НД ТЗІ 3.1-001-07.

2. Характеристика ОІД.

ОІД – приміщення, що розташоване на 1 поверсі адміністративного будинку за адресою: м. Київ вул. Ахматової 12. Вікно приміщення ОІД виходять з заходу Районний відділ комісаріату, зі сходу Дитячий садок, з півдня смітник, з півночі склад «Нова пошта». Межі контрольованої зони об’єкта (мал. 2.1) співпадають із контрольованою зоною, у якому розташований ОІД.



Мал. 2.1. Ситуаційний план

3. Характеристика складових ОІД

Приміщення ТОВ «Радар» призначено для обробки інформації, що становить державну або іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави, або вимога щодо захисту якої встановлено законом (далі - інформації з обмеженим доступом). Режим обробки інформації – реального часу.

Архітектурно-будівельні особливості приміщення товщина стін 300мм.

– в приміщені розташовано дерев’яні двері з двома замками.

У суміжних приміщеннях ІзОД не циркулює. З обох сторін знаходяться приміщення для нарад і склад речей

В суміжних приміщеннях, та в будинку без належного контролю не працюють іноземні громадяни, неконтрольоване перебування сторонніх осіб унеможливлено (Довідка № 30118-7 ДСК від 11.10.2016).

Складові ОІД, що можуть впливати на показники ефективності захищеності ІзОД і які можуть бути середовищем поширення за межі КЗ її носіїв (інженерні комунікації, обладнання, оргтехніка, засоби ТЗІ (за наявності), пожежна, охоронна сигналізації, телебачення, системи зв’язку, радіофікації, часофікації, автоматизації, керування, електроживлення, заземлення, газо-, водопостачання, опалення, вентиляції, кондиціонування повітря, водостоку, каналізації, технологічне

обладнання, огороджувальні будівельні конструкції, світлопроникні отвори приміщень, будинків, споруд, салонів транспортних засобів тощо):

Система охоронної сигналізації встановлена на вікнах і дверях. Головний пульт керування знаходяться у межах КЗ.

Приміщення обладнано системою пожежної сигналізації. В кімнаті знаходяться 2 датчики.

Система заземлення підключення до місцевої мережі і знаходяться у мережі КЗ.

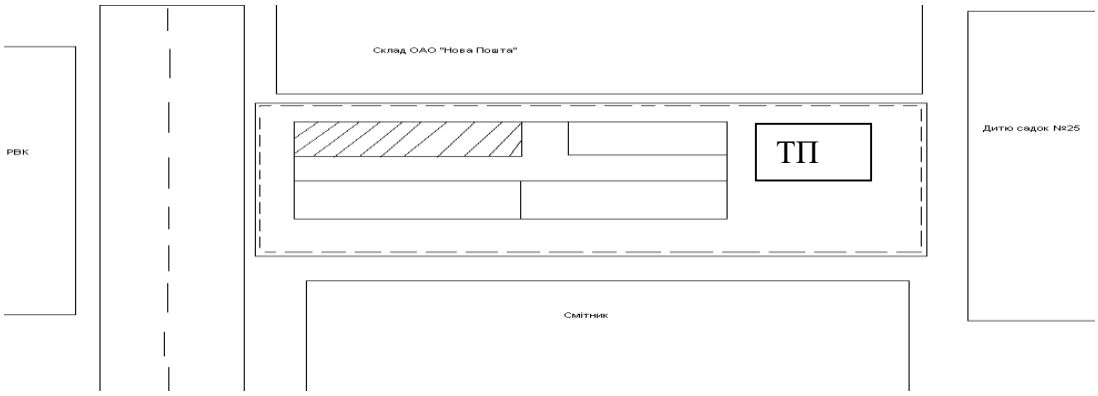
Система опалення автономне і знаходяться у межах КЗ.

Система водопостачання автономне і знаходяться у межах КЗ.

Система водостоку не підключення до центральної міської каналізації і не аєв межах КЗ.

4. Схеми розміщення комунікацій, обладнання систем електроживлення, у т.ч. трансформаторної підстанції.

Електроживлення – знижувальна трансформаторна підстанція, від якої живляться ОТЗ і ДТЗС, знаходиться в межах КЗ.



Мал. 2.2 Генеральний план ТОВ «Радар» вул. Ахматової 12

5. Результати аналізу наявності в установі:

затверджена схема КЗ (від 11.06.2017) в межах якої розташований ОІД;

дані про можливі місця розміщення зовні КЗ засобів технічної розвідки тривалого перехоплення зазначені в Окремій моделі загроз для ОІД;

дані за результатами проведення випробувань (у т.ч. спеціальних досліджень технічних засобів, які обробляють ІзОД) будуть зазначені у відповідному протоколі випробувань.

6. Данні щодо терміну проведення категоріювання об'єктів та подання на затвердження актів із категоріювання:

Акт категоріювання ОІД ТОВ «Радар» вул. Ахматової 12 кімната №201 (обл. № 112 дск від 11.03.2015).

голова комісії Смірнов В.А.

члени: Сорокін В.Д. _____

Курков С.С _____

2.3. Розробка акту категоріювання об’єкту інформаційної діяльності

Для службового користування
(після заповнення)
Прим. № _1
ЗАТВЕРДЖЕНО
Ген. Дир.
Коваленко А.С.
3.03.17

АКТ № 12

«категоріювання кімнати №101 для роботи з інформацією з грифом «цілком таємно»

3.03.17 м. Київ

Комісія у складі:

голова Смірнов В. А. – начальник

члени: Сорокін В.Д. – нач. РСО

Курков С. С. – зам. нач. РСО

Призначена наказом №1 від 13.03.2016 провела категоріювання кімнати для нарад №3.

Категоріювання проводиться у зв’язку з тим, що система ТЗІ для даного ОІД розробляється і впроваджується вперше.

Комісія розглянула та проаналізувала:

-ситуаційний план

-генеральний план -схеми електроживлення

-схеми комунікацій, що мають вихід за межі КЗ

Комісія постановила:

1. В кімнаті для роботи з інформацією №101 де циркулює така інформація:

2.1 Мовна інформація (під час занять) вголос, під час розмов між співробітниками цього підприємства. Гриф –таємно**.**

2.2 Інформація в ПЕОМ. Гриф обмеження доступу – цілком таємно

2. Приміщенню, де циркулює ІзОД та під час розмов між співробітниками цього підприємства, присвоїти другу категорію.
3. У наявності всі НД ТЗІ

Додатки:

1. Ситуаційний план (додаток 1)
2. Генеральний план (додаток 2)
3. Схеми комунікацій, що мають вихід за межі КЗ
4. План розташування ОТЗ та ДТЗС на ОІД

Кількість примірників - 1

Комісія в складі:

голова Смірнов В. А. – начальник _____

члени: Сорокін В. Д. начальник РСО _____

Курков С. С. – зам. нач. РСО … _____

2.4. Розробка політики інформаційної безпеки

Загальні положення.

Політика безпеки визначає норми, правила і обмеження по користуванню елементами інформаційної системи, є механізмом управління інформаційною системою.

Відповідальним за безпеку інформації завжди є керівник організації.

Керівник може призначати конкретних працівників відповідальними за безпеку окремих елементів інформаційної системи.

Всі працівники повинні ознайомитись з даним документом та безвідмовно дотримуватись всіх нижчезазначених правил, обов’язків та вимог.

Політика безпеки висвітлює лише загальні та обов’язкові положення безпеки організації. Всі деталі повинні вирішуватись персоналом організації згідно з їх обов’язками, посадовими інструкціями та практичними навичками і досвідом. (напр. видача прав доступу працівникам, генерування паролів, застосування шифрування, використання програмного забезпечення, охоронних сигналізації і т.д.)

Політика інформаційної безпеки в АС - 1

Таблиця 2.1.

№ пп	Положення ПІБ	Відповідальні особи
	Організація захисту	
1.	Регулярно проводити наради з персоналом, на яких варто розглядати наступні питання: Аналіз та затвердження (внесення змін при необхідності) до політики безпеки і розподіл загальних обов'язків Визначення основних загроз інформаційних ресурсів Визначення та затвердження дій, спрямованих на покращення захисту інформації	Керівник, група режиму, аналітична група
2.	Узгоджуються конкретні функції і обов'язки по забезпеченню інформаційної безпеки Узгоджуються конкретні методики і процеси захисту інформації (напр. оцінка ризиків, система класифікації методів захисту) Узгоджується і здійснюється підтримка ініціатив з захисту інформації (напр. програма навчання персоналу правилам безпеки)	Керівник СБ
3.	Всі прийняті рішення стосовно інформаційної безпеки організації повинні узгоджуватись керівником організації.	Керівник
	Класифікація ресурсів і їх контроль	
1.	Всі основні інформаційні ресурси організації повинні мати власника. Власник затверджується керівником організації.	Керівник, група режиму
2.	Відповідальним за безпеку інформаційного ресурсу завжди є його власник.	Група режиму
3.	Власник ресурсу може призначати також відповідальним за безпеку ресурсу іншу особу (затверджується керівником та СБ)	Група режиму
4.	Не рідше ніж один раз в пів року проводити інвентаризацію всіх ресурсів організації. При цьому виконуються наступні дії: Кожен ресурс повинен бути чітко ідентифікований Власник ресурсу та відповідальні за безпеку особи визначені	СБ
	Безпека персоналу	
1.	При прийомі працівників на роботу необхідно ретельно перевіряти достовірність інформації, вказаної в заявах та анкетах.	Детективна група
2.	Працівники, що мають доступ до конфіденційної інформації повинні підписати документи про нерозголошення таємниць.	Група режиму
3.	Документи про нерозголошення інформації повинні переглядатись та при необхідності змінюватись при зміні грифів таємності та класифікації інформації.	Група режиму

4.	Необхідно навчити працівників процедурам захисту і правильному поводженню з інформаційними ресурсами.	Група режиму
	Фізична безпека системи	
1.	При прийомі на роботу працівників, їх права на доступ в приміщення організації повинні бути чітко визначені, затверджені і задокументовані. Працівникам необхідно видати персональні ідентифікаційні картки, картки та коди доступу в відповідні приміщення.	Детективна група, група режиму, керівник
2.	Дата та час приходу працівників на роботу та залишення контрольованої території повинен реєструватись в системному журналі на КПП.	Служба охорони
3.	Дата та час входу в приміщення повинен реєструватись в системному журналі через електронні замки.	Група режиму
4.	Працівники повинні завжди носити на видному місці особисті ідентифікаційні картки.	Служба охорони
5.	При помічені в приміщенні сторонніх осіб чи осіб, що не мають прав доступу до приміщення необхідно негайно повідомити про це службу охорони з допомогою кнопки тривоги чи в усній формі.	Служба охорони
6.	При звільненні працівників необхідно вилучити у них особисті ідентифікаційні картки, картки та коди доступу до приміщень.	Група режиму
7.	Забороняється зберігати вогненебезпечні та легкозаймисті предмети близько біля життєвоважливих ресурсів системи (комп'ютерів, сигналізації, систем контролю доступу і т.і.)	Група пожежної охорони, служба охорони
8.	При покиданні приміщення чи роботі в приміщенні з таємною інформацією слід закривати вікна та двері та ретельно перевіряти безпеку системи.	Група режиму, працівники
9.	Магнітні носії інформації та паперову документацію, коли вони не використовуються, слід зберігати в спеціаних захищених шафах.	Працівники
10.	Коли комп'ютери не використовуються слід їх виключати або блокувати паролем систему.	Працівники
11.	Працівникам категорично забороняється виносити будь-яке майно організації за її межі.	Служба охорони
12.	Працівникам категорично забороняється приносити будь які сторонні предмети на територію організації.	Служба охорони
13.	Необхідно регулярно перевіряти стан електромережі та дотримання всіх правил користування електроапаратурою.	Електрик
14.	Технічне обслуговування повинен здійснювати технічний персонал служби підтримки апаратури під наглядом СБ.	Група режиму
15.	Не рідше ніж один раз в пів року слід оглядати всю апаратуру.	Інженери, адміністратор, група режиму
16.	Ретельно перевіряти магнітні носії, що не використовуються, по таким пунктам: Наявність записаної на них таємної інформації Наявність пошкоджень	Група режиму, аналітична група

Продовження таблиці 2.1

	Робото спроможність	
17.	В разі виявлення таємної інформації на МНІ слід її видалити.	Група режиму
18.	В разі виявлення пошкоджень МНІ або нероботоспроможність МНІ утилізувати.	Група режиму
19.	Регулярно (раз в тиждень) проводити перевірку приміщень та території на наявність закладних пристроїв.	Група протидії технічним розвідкам, аналітична група
20.	Необхідно регулярно перевіряти стан пожежної сигналізації.	Група пожежної охорони.
21.	Необхідно регулярно перевіряти стан систем контролю доступу до приміщень.	Група режиму
22.	Необхідно регулярно загальні засади захисту інформації, аналізувати та давати точну оцінку стану системі безпеки організації.	Аналітична група.

2.5. Розробка моделі загроз інформаційній безпеці

Для службового користування
(після заповнення)
Прим. № _1
ЗАТВЕРДЖЕНО
Ген. Дир.
Коваленко А.С.
МП
«___»
_____2017р.

ТОВ ”Радар”
(ПРИМІЩЕННЯ № 101)
МОДЕЛЬ ЗАГРОЗ
для інформації з обмеженим доступом, яка циркулює на об’єкті інформаційної діяльності
2018

Таблиця 2.2.

Зведена таблиця моделі загроз

№ п/п	Перелік суттєвих загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз	Наслідки (порушення властивостей)			
				К	Ц	Д	
1	Виведення з ладу технічних засобів	Персонал, користувачі ТЗ, сторонні особи, які отримали несанкціонований доступ	Фізичний НСД до обладнання, що захищається		+	+	

2	Порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації)	Персонал, користувачі, сторонні особи, ТЗ	Фізичний НСД до обладнання, що захищається		+		
3	Порушення режимів функціонування АС (обладнання і ПЗ) та систем життєзабезпечення АС	Персонал, користувачі, сторонні особи, ТЗ	Фізичний НСД до обладнання, що захищається, застосування ЗП, програм, комп'ютерних вірусів		+		
4	Незаконне підключення: до апаратури, системи електроживлення, заземлення, життєзабезпечення	Персонал, користувачі, сторонні особи, ТЗ	Фізичне підключення	+	+	+	+
5	Читання "сміття" (залишкової інформації з запам'ятовуючих пристроїв, магнітних аудіо касет)	Персонал, користувачі, сторонні особи, ТЗ, ПЗ	НСД до МНСІ або оперативної пам'яті сторонніх осіб, застосування ЗП, програм	+			
6	Читання даних, що виводяться на екран, роздруковуються, встановлення мікро аудіо-відео записуючих пристроїв, читання залишених без догляду віддрукованих на принтері документів	Персонал, користувачі, відвідувачі, сторонні особи	Знаходження сторонніх осіб в службових приміщеннях	+	+	+	+
7	Несанкціоноване використаня технічних пристроїв	Персонал, користувачі, відвідувачі, сторонні особи	Фізичний НСД до обладнання, що захищається	+	+	+	+
8	Несанкціоноване внесення змін (підміни) в КТЗІ, в програмне забезпечення, в компоненти інформаційного забезпечення	Персонал, користувачі, відвідувачі, сторонні особи	Фізичний НСД до обладнання та ПЗ, подолання заходів захисту	+			+
9	Несанкціоноване копіювання вихідних документів, магнітних та інших носіїв інформації (у тому числі при проведенні ремонтних та регламентних робіт)	Персонал, користувачі, відвідувачі, сторонні особи	НСД до МНСІ , подолання заходів захисту, застосування ЗП, комп'ютерних вірусів	+			
10	Розкрадання магнітних носіїв, документів,	Персонал, користувачі,	НСД в приміщення, до	+		+	

	чернеток, отримання не облікованих копій	відвідувачі,	технічних засобів				
12	Впровадження і використання комп'ютерних вірусів	Персонал, користувачі, відвідувачі, сторонні особи, ПЗ	Фізичний НСД до обладнання та ПЗ, подолання заходів захисту	+	+	+	+

Продовження таблиці 2.2

2.6. Розробка моделі порушника інформаційної безпеки

Порушник – це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

Відносно АС 1 порушники можуть бути внутрішніми (з числа персоналу або користувачів системи) або зовнішніми (сторонніми особами). Визначення категорії порушників, прийнятих в моделі, приведено у таблиці 2. В таблицях 3-7 наведені специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо АС 1, за показником можливостей використання засобів та методів подолання системи захисту, за часом дії, за містом дії. У графі "Рівень загроз" зазначених таблиць наведені у вигляді відносного ранжування оцінки можливих збитків, які може заподіяти порушник за умови наявності відповідних характеристик. Рівень збитків характеризується наступними категоріями:

1 - незначні, 2 – значимі, але, здебільшого, припустимі, 3 – середні, 4 – дуже значні.

Таблиця 2.3

Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загрози
	Внутрішні по відношенню до АС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, сантехніки, прибиральники тощо), в яких розташовані компоненти АС	1
ПВ2	Персонал, який обслуговує технічні засоби (інженери, техніки)	2
ПВ3	Користувачі (оператори) АС	2
ПВ4	Співробітники підрозділів (підприємств) розробки та супроводження програмного забезпечення	3
ПВ5	Адміністратори ЛОМ	3
ПВ6	Співробітники служби захисту інформації	4
ПВ7	Керівники різних рівнів посадової ієрархії	4
	Зовнішні по відношенню до АС	
ПЗ1	Будь-яки особи, що знаходяться за межами контрольованої зони.	1
ПЗ2	Відвідувачі (запрошені з деякого приводу)	2
ПЗ3	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ4	Хакери	3
ПЗ5	Співробітники закордонних спецслужб або особи, які діють за їх завданням	4

Таблиця 2.4

Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	1
М2	Самозатвердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок	4

Таблиця 2.5

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо АС 1

Позначення	Основні кваліфікаційні ознаки порушника	Рівень

		загрози
К1	Знає функціональ ...кономірності формування масивів даних та ...ички щодо користування штатними засобами системи	1
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем	2
К4	Знає структуру, функції й механізми дії засобів захисту, їх недоліки	3
К5	Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його недокументовані можливості	3
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення	4

Продовження таблиці 2.5

Таблиця 2.6

Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Використовує лише агентурні методи одержання відомостей	1
З2	Використовує пасивні засоби (технічні засоби переймання без модифікації компонентів системи)	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв’язку) упровадження програмних закладок та спеціальних резидентних програм збору, пересилання або блокування даних, дезорганізації систем обробки інформації.	3
З5	Застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних).	4

Таблиця 2.7.

Специфікація моделі порушника за місцем дії.

Позначення	Характеристика місця дії порушника Продовження таблиці 2.7	Рівень загрози
Д1	Без доступу на контрольовану територію організації	1
Д2	З контрольованої території без доступу у будинки та споруди	1
Д3	Усередині приміщень, але без доступу до технічних засобів АС	2
Д4	З робочих місць користувачів (операторів) АС	2
Д5	З доступом у зони даних (баз даних, архівів й т.ін.)	3
Д6	З доступом у зону керування засобами забезпечення безпеки АС	4

Для побудови даної моделі використаємо усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них вказується в дужках і оцінюється за 4-бальною шкалою.

Визначення категорії

Мотив порушення

Рівень кваліфікації та обізнаності щодо АС .

Можливості використання засобів та методів подолання системи захисту.

Специфікація моделі порушника за часом дії

Специфікація моделі порушника за місцем дії

Сумарний рівень загрози

2.7. Розробка технічного завдання на створення КСЗІ в АС 1

УЗГОДЖЕНО	ЗАТВЕРДЖУЮ
…….	…….
…….	…….
М.П.	М.П.
"_____"_____ 2018 р.	"_____"_____ 20 18 р.

АВТОМАТИЗОВАНА СИСТЕМА
ТОВ РАДАР

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Технічне завдання

Київ – 2018 р.

З М І С Т

1 Перелік скорочень

АРМ - автоматизоване робоче місце;

АС - автоматизована система;

ЕОТ - електронно-обчислювальна техніка;

ІзОД - інформація з обмеженим доступом;

КЗЗ - комплекс засобів захисту;

КЗІ - криптографічний захист інформації;

КСЗІ - комплексна система захисту інформації;

ЛОМ - локальна обчислювальна мережа;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД - несанкціонований доступ;

ОС - операційна система;

ПЗ - програмне забезпечення;

ТЗ - технічне завдання;

2 Терміни та визначення

У цьому ТЗ використовуються терміни та визначення згідно з ДСТУ 3396.2-97, ДСТУ, НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу", а також такі терміни та визначення: Загальні відомості

Це технічне завдання визначає вимоги до комплексу організаційних та технічних заходів щодо забезпечення захисту інформації в автоматизованій системі (АС 1) ТОВ Радар

Умовне позначення АС1

Шифр: AF Договір: #775

Замовник – ТОВ Радар

Початок робіт: 6.06.2018 Закінчення: 06.06.2018

Підстава для розробки: Реформування та профілактика заходів безпеки

Фінансування роботи здійснюється за рахунок ТОВ Радар

Технічне завдання на комплексну систему захисту інформації оформлено відповідно до ГОСТ 34.601-90 та ГОСТ 34.602-86 .

2.7. Загальні відомості

1. Повна назва роботи, автоматизована система ТОВ Радар комплексна система захисту інформації

1.1.1. Повна назва роботи: "Розробка комплексної системи захисту інформації в автоматизованій інформаційній системі 1 ТОВ Радар.

1.1.2. Шифр роботи – КСЗІ ТОВ Радар.

1.2 Назва підприємства-розробника підсистеми та його реквізити

1.2.1 ТОВ Праймус,

М. Київ Вул. Лукашенко 4 ,

Рахунок: (145588254)р/р 4568476478 в 4548648у м. 48648684 МФО 1534834 .

1.2.2. Спеціальний дозвіл на впровадження діяльності з державною таємницею, від 2012 року, №745 , дійсний до 2020року;

Ліцензія серія ТТ № 5698563 Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України або Державної Служби

спеціального зв’язку та захисту інформації України. Дата видачі 12,12,2010 . Строк дії з 12,12,2010 до 2020 року.

1.3. Назва замовника роботи та його *реквізити*:

Товариство з обмеженою відповідальність Радар

Рахунок: код 65463 , р/р 8453143 в 851464 у м. 8431 МФО 46468446 .

1.4 Планові терміни початку і закінчення роботи зі створення КСЗІ

Початок – 10,12,2017 року.

Закінчення – 12,12,2018 року.

1.5. Порядок оформлення і надання Замовнику результатів робіт

1.5.1. Порядок виконання і приймання стадій і етапів робіт встановлюється з урахуванням вимог ГОСТ 34.601-90 та ГОСТ 34.602-86.

1.5.2 За результатами проведених робіт Виконавець щороку подає Замовнику робіт акт здачі-приймання робіт, який містить заключний звіт про виконані роботи та кошторис фактичних витрат за формами, що визначені Положенням про порядок формування цільових програм наукових досліджень ТОВ Мегатрон, затвердженим розпорядженням Президії ТОВ Мегатрон від 25 листопада 2013 р. № 682.

1.5.3. Склад та зміст документів, що розробляються, визначається з урахуванням вимог ГОСТ 34.201-89 та нормативних документів системи ТЗІ.

4. Мета і призначення комплексної системи захисту інформації

Метою створення комплексної системи захисту інформації є забезпечення безпеки критичної інформації в процесі оброблення її засобами АС ІзОД . Захист інформації повинен забезпечуватися на всіх технологічних етапах обробки критичної інформації і в усіх режимах функціонування.

Процес оброблення інформації складається з таких технологічних етапів:

формалізації первинної інформації, одержаної від ТОВ Радар та зберігання її в локальних базах даних у вигляді блоків даних;

використання формалізованої, накопиченої ТОВ Праймус

обміну блоками даних між окремими автоматизованими робочими місцями та локальними АС1 каналами структурованої кабельної системи передачі даних під час роботи

Для забезпечення безпеки інформації на всіх стадіях життєвого циклу АС 1 комплексна система захисту інформації передбачає застосування таких заходів та засобів захисту інформації:

організаційні заходи, що реалізуються поза обчислювальною системою АС1;

програмно-апаратні засоби захисту від несанкціонованого доступу;

запобігання витоку інформації технічними каналами;

захисту інформації під час передавання/приймання її каналами зв'язку;

КСЗІ в АС 1 призначена для:

захисту інформації з обмеженим доступом від витоку її технічними каналами;

керування доступом користувачів до інформаційних ресурсів АС1;

розмежування доступу користувачів АС 1 до інформації різних категорій конфіденційності;

блокування несанкціонованих дій з критичною інформацією;

створення багаторівневого захисту інформаційних ресурсів АС 1 від атак;

контролю та захисту внутрішніх і зовнішніх потоків інформації, яка обробляється розподіленою обчислювальною системою АС 1;

реєстрації спроб реалізації загроз інформації та оперативного сповіщення адміністраторів безпеки про факти несанкціонованих дій з інформацією обмеженого доступу;

Нормативно-правовою базою щодо захисту інформації та створення КТЗІ АС 1 є Закони України "Про інформацію", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах".

5.Нормативно-правові акти, затверджені Указами Президента України та постановами Кабінету Міністрів України:

Положення про технічний захист інформації в Україні. Затверджено Указом Президента від 27.09.99 р. №1129;

Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 8 жовтня 1997 року № 1126;

Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Затверджено постановою Кабінету Міністрів України від 16.02.98 № 180;

«Порядок організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях», затверджено постановою Кабінету Міністрів України від 2 жовтня 2003 р. № 1561-12.

Державні стандарти та інші нормативні документи з стандартизації:

ДСТУ 3396.0-96. Технічний захист інформації. Основні положення.

ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт.

Нормативні документи системи технічного захисту інформації в Україні:

ТПКО-95. Тимчасове положення про категоріювання об'єктів. Затверджено наказом ДСТЗІ від 10 липня 1995 року № 35;

НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ від 28 квітня 1999 року №22.

НД ТЗІ 2.5-007-2001. Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу 1. Затверджено наказом ДСТСЗІ СБУ від 18 червня 2001 року № 05.

НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ від 20 грудня 2000 року № 60.

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. за №22.

НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБУ від 9 лютого 2001 року № 2.

НД ТЗІ 1.6-003-2004 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розробки, побудови, викладення та оформлення моделі загроз для інформації. Затверджено наказом ДСТСЗІ СБУ від 04 січня 2004 року.

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в АС, Затверджено наказом ДСТЗІ СБУ від 4 грудня 2000 року №53.

НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБУ від 08 листопада 2005 року № 125.

Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами ПЕМВН (ТР ЕОТ-95), затверджене наказом ДСТЗІ від 09.06.95 р. №25.

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМ від 29 березня 2006 р. № 373.

1. Загальна характеристика АС та умови функціонування

Призначення АС:

автоматизація обробки інформації обробки матеріалів в галузі військового текстилю

Найвищий гриф інформації, що буде оброблятися засобами АС та передаватися каналами зв’язку, - ЦТ

Режим обробки інформації з найвищим грифом:

при ЦТ - постійний;

До складу АС 1 входять:

головний інформаційно-аналітичний підрозділ №1

інформаційно-аналітичні підрозділи №1

Інформаційний ресурс АС являє собою БД. При цьому необхідні і достатні для вирішення завдань щодо забезпечення БД . У складі АС виконують функції збору, формалізації, накопичення, обробки та передачі інформації.

Принципи організації інформаційних зв’язків АС

АС1 сприймає на себе і контролює всі вихідні інформаційні потоки від БД які організаційно і функціонально залежать від даного рівня управління;

БД – є джерелом інформації для АС

Базовими елементами АС є автоматизовані робочі місця, що повинні забезпечувати постачання частково формалізованої та структурно упорядкованої (уніфікованої) первинної інформації для БД.

Комунікаційні засоби функціональних вузлів працюють цілодобово без вимкнення живлення (2 годин на добу з подальшим вимкненням живлення). Технічні засоби АРМ функціональних вузлів допускають їх цілодобову роботу без вимкнення живлення (8 годин на добу з подальшим вимкненням живлення).

Базове програмне забезпечення АРМ складається з:

мережевої операційної системи Win 10 ;

системи керування базами даних MS Exel ;

Вимоги до комплексної системи захисту інформації

Загальні вимоги.

Архітектура АС повинна дозволяти розв’язання функціональних завдань у замкненому середовищі. Структура мережі, розподіл потоків даних повинні забезпечувати мінімально можливий час передачі критичної інформації між локальними сегментами мережі.

Робота АС у штатних режимах повинна бути можливою лише за умови функціонування системи захисту інформації.

Розташування, монтаж та прокладку інженерно-технічних комунікацій АС, в тому числі систем заземлення та електроживлення технічних засобів, які приймають участь у обробці інформації, необхідно виконувати з дотриманням вимог відповідних стандартів та нормативних документів системи ТЗІ.

Організаційні та підготовчі заходи щодо технічного захисту інформації повинні проводитися одночасно і складати перший етап робіт зі створення КТЗІ, на якому повинні бути виявлені потенційні загрози безпеці інформації.

Під час проведення обстеження приміщень, технічних засобів та систем забезпечення інформаційної діяльності АС необхідно, по-перше, виконати роботи з дослідження можливостей витоку інформації внаслідок роботи основних технічних засобів перетворення (обробки, зберігання, відображення) інформації, (ТЗПІ) та допоміжних технічних засобів та систем (ДТЗС). (Конкретний перелік ТЗПІ та ДТЗС надається Замовником).

По-друге, як джерела витоку ІзОД також повинні бути розглянуті ланки передачі інформації, ланки електроживлення, заземлення, керування та сигналізації, а також ланки, створені паразитними зв'язками, конструктивними елементами будівель, споруд, устаткування та інше.

По-третє, необхідно провести дослідження засобів обчислювальної техніки, які формують, передають, приймають, перетворюють, відображають та зберігають ІзОД, щодо наявності технічних каналів витоку інформації шляхом побічних електромагнітних випромінювань та наводок (ПЕМВН).

Неформалізована модель загроз для інформації (додається), яка розроблена із врахуванням результатів обстеження приміщень, технічних засобів та систем забезпечення інформаційної діяльності АС, включає:

ситуаційний план розташування структурних елементів АС із зазначенням місць розташування технічних засобів та систем обробки інформації і життєзабезпечення, джерел електроживлення, контурів заземлення, енергетичних

мереж, а також інженерних комунікацій, що виходять за межі зони безпеки інформації;

опис можливих технічних каналів витоку інформації та впливу на неї;

опис можливих способів реалізації несанкціонованого доступу до інформації;

оцінку обсягів можливих збитків від реалізації загроз безпеці інформації;

Для реалізації частини політики безпеки інформації, яка покладається на технічні заходи і відповідає реальній моделі загроз, КЗЗ повинен мати такі функціональні можливості:

забезпечення входу в систему та завантаження операційної системи на робочій станції за умови пред'явлення електронного ідентифікатора і/або введення особистого паролю;

контроль за вводом інформації в АС та інсталяцією програмного забезпечення;

контроль за виведенням інформації на носії, що вилучаються;

підтримка функцій адміністратора захисту інформації в АС;

реєстрація дій користувачів по відношенню до ресурсів системи;

забезпечення цілісності інформаційних ресурсів (у тому числі і антивірусний захист);

перевірка цілісності та роботоздатності КТЗІ;

надання користувачам прав доступу до ресурсів АС згідно прийнятої політики безпеки, та їх ліквідація по закінченню строку дії;

багаторівневе розмежування повноважень персоналу АС по відношенню до ресурсів АС;

контроль за запуском процесів та їх виконанням;

автоматичне блокування екрану робочої станції на час відсутності користувача;

заборона роботи зареєстрованим користувачам у невідведений час;

шифрування інформації, автентифікація повідомлень і підтвердження їх походження при передачі каналами зв'язку;

Виконання завдань повинне здійснюватися зареєстрованими користувачами у функціонально замкненому середовищі із забезпеченням доступу до ресурсів, що обмежені рамками завдань.

Програмне забезпечення АРМ користувачів повинне містити програмні модулі захисту, що забезпечують взаємодію із сервером захисту для реалізації функціональних послуг безпеки.

Для керування КТЗІ у складі АС повинно бути передбачено АРМ адміністратора безпеки. Аналогічні АРМ повинні включатися до складу віддалених сегментів АС. Вказані АРМ (а також сервери захисту та інші мережні сервери) повинні розташовуватися у виділених приміщеннях із дотриманням необхідних організаційних заходів.

Введення інформації з магнітних носіїв, де це технологічно необхідно, має здійснюватися на виділених робочих місцях, із вжиттям відповідних організаційних заходів.

КСЗІ повинна забезпечувати підтримку:

не менше 2 категорій таємності інформації;

не менше 3 рівнів повноважень користувачів;

роботи не менше 5 користувачів та 25груп користувачів.

Комплексна система захисту інформації повинна реалізовуватися як сукупність узгоджених за часом та місцем застосування організаційних, підготовчих технічних і технічних заходів.

Організаційні заходи повинні включати:

визначення та встановлення обов’язків із захисту інформації підрозділів та осіб, що приймають участь в обробці інформації;

визначення технологічних процесів обробки інформації з урахуванням вимог із захисту інформації;

встановлення порядку впровадження та модернізації засобів обробки інформації, програмних та технічних засобів захисту інформації;

організацію фізичного та протипожежного захисту АС;

розробку правил та порядку контролю функціонування КТЗІ;

Під час створення КЗЗ для забезпечення вимог щодо захисту інформації повинні використовуватися засоби технічного захисту інформаціїї з "Переліку засобів технічного захисту інформації загального призначення", затвердженого ДСТСЗІ СБ України або розроблятися та реалізовуватися спеціальні засоби ТЗІ, як невід'ємна частина АС .

Вимоги до функціональних послуг

КЗЗ КТЗІ установи ТОВ Альтрону відповідності до вимог НД ТЗІ 2.5-005 -99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" повинен реалізовувати наступний профіль захищеності інформації:

2.КЦД.2 = { КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }.

Вимоги до гарантій

У відповідності з рекомендаціями документу "Технічне завдання на створення типової комплексної системи захисту інформації" рівень гарантій реалізації визначеного функціонального профілю захищеності АІС установи ТОВ Альтрон має бути не нижчим за Г2 (згідно з вимогами НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»).

6.3.1 Вимоги до гарантій архітектури КЗЗ

КЗЗ повинен складатися із добре визначених і максимально незалежних компонентів. Кожний із компонентів повинен бути спроектований виходячи із принципу мінімуму повноважень. Архітектура КЗЗ повинна бути побудована за принципом відкритих систем і передбачати можливість реалізації додаткових послуг безпеки інформації в частині захисту від несанкціонованого доступу.

6.3.2 Вимоги до гарантій середовища опрацювання

Розробник повинен розробити і впровадити документовані методики по управлінню конфігурацією комплексу засобів захисту на всіх стадіях життєвого циклу АС. Система управління конфігурацією повинна забезпечувати управління внесенням змін в програмне забезпечення і документацію.

Додаткові програмні засоби захисту інформації необхідно розробляти в середовищі сучасних засобів розробки програм під Windows з використанням сучасної та документованої мови програмування.

Програмні засоби слід розробляти з використанням будь-якого із сучасних засобів розробки прикладних програм для ОС Windows, в якому використовується добре визначена документована мова програмування.

Керування конфігурацією повинно здійснюватися на основі базових версій – версія КЗЗ, яка може бути змінена тільки через формальні процедури зміни.

Елементами КЗЗ, конфігурація яких підлягає керуванню, є програмні засоби, що входять до складу КЗЗ, настройки КЗЗ та документація.

Зміни в елементи конфігурації повинні вноситися на основі узгоджених організаційних документів у результаті приймання етапів робіт зі створення КТЗІ, проведення випробувань та дослідної експлуатації.

6.3.3 Вимоги до гарантій проектування

Процес створення КЗЗ повинен передбачати наступні етапи:

Попередній етап:

проведення обстеження ОІД;

визначення переліку загроз і можливих каналів витоку інформації;

визначення вимог до КЗЗ;

розробка технічного завдання.

Етап проектування і розробки КЗЗ:

вибір необхідних настроювань КЗЗ;

вибір і настроювання сервісів безпеки ОС та антивірусного ПЗ;

інсталяція та настроювання засобів захисту БД;

розробка відповідної документації.

Етап випробувань і передачі КЗЗ в експлуатацію:

проведення попередніх випробувань КЗЗ у складі КТЗІ;

проведення дослідної експлуатації КЗЗ у складі КТЗІ;

державна експертиза КЗЗ у складі КТЗІ.

6.3.4 Вимоги до гарантій середовища функціонування

Розробник повинен надати засоби інсталяції, генерації та запуску КЗЗ, які гарантують, що експлуатація починається із безпечного стану. Під час розробки КЗЗ повинні бути описані необхідні настройки та параметри конфігурації, які можуть використовуватися у процесі інсталяції, генерації та запуску КЗЗ і дозволяють розпочати функціонування починаючи з безпечного стану.

6.3.5 Вимоги до гарантій експлуатаційної документації

Експлуатаційна документація на КЗЗ повинна включати загальний опис КЗЗ, настанови адміністратора системи та користувача, а також експлуатаційну документацію виробників на покупні вироби, що входять до складу КЗЗ. Повний склад документації наведено в розділі 5 даного Технічного завдання.

6.3.6 Вимоги до гарантій випробувань комплексу засобів захисту

Випробування КЗЗ повинні проводитися згідно «Програми та методики випробувань», яка повинна містити процедури перевірки всіх заявлених послуг безпеки.

6.5 Вимоги до КТЗІ в частині захисту від витоку технічними каналами

Можливими технічними каналами витоку інформації є витік інформації за рахунок побічних електромагнітних випромінювань та наведень (ПЕВМН), а також акустичного та візуально оптичного каналу.

6.5.1 Вимоги до системи електроживлення АС

1. Електроживлення АІС установи ТОВ Мегатрон повинне здійснюватися від трансформаторної підстанції низької напруги, розміщеної у межах контрольованої території. У випадку знаходження трансформаторної підстанції за межами контрольованої території електроживлення повинно здійснюватися через розділовий трансформатор.

2. Мережа електроживлення АІС установи ТОВ Альтрон повинна бути відділена від мережі освітлення та побутової мережі і забезпечувати безперебійну експлуатацію та працездатність ТОВ Альтрон.

3. Електроживлення повинно здійснюватися через протизавадні мережеві фільтри.

6.5.2 Вимоги до кіл заземлення АС 1

1. Усі металеві конструкції ОТЗ повинні бути заземлені.

2. Система заземлення не повинна мати вихід за межі контрольованої території.

3. Опір кіл заземлення від засобів ТОВ Радар до вузлів системи заземлення не повинен перевищувати 4 Ом.

4. Для системи заземлення ТОВ Радар не повинні використовуватися природні заземлювачі (металеві трубопроводи, залізобетонні конструкції будинків тощо).

6.5.3 Вимоги до структурованої кабельної мережі АС

Вимоги до захищеності інформації від витоку технічними каналами визначаються на підставі НД ТЗІ ТР ЕОТ-95 “Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок” і ТР ПЕМВН-95 “Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок",

Зміст та послідовність робіт з протидії загрозам витоку інформації технічними каналами повинні відповідати зазначеним в ДСТУ 3396.0-96, ДСТУ 3396.1-96 етапам:

1 етап – проведення обстеження об’єкта інформаційної діяльності, визначення і аналіз загроз, розроблення моделі загроз;

2 етап – розроблення комплексу технічного захисту інформації від витоку технічними каналами;

3 етап – реалізація комплексу технічного захисту інформації;

4 етап – спецдослідження об’єкта інформаційної діяльності, оцінка якості та надійності технічного захисту інформації від витоку технічними каналами, видача приписів на експлуатацію.

Конкретизація заходів та засобів захисту інформації від витоку інформації технічними каналами повинна бути здійснена при проведенні спецдосліджень об’єкту інформаційної діяльності.

7 Вимоги до складу проектної та експлуатаційної документації

До складу документації на КТЗІ, що розробляються виконавцем ДКР, повинні входити:

загальний опис КТЗІ;

паспорт - формуляр ТОВ Мегатрон;

акт обстеження об’єкта інформаційної діяльноі

модель загроз об’єкту інформаційної діяльності;

протоколи спецдосліджень ПЕОМ та інших ОТЗ;

припис на експлуатацію;

настанови адміністратора системи (в частині КТЗІ);

настанови адміністратора безпеки (в частині КТЗІ);

настанови адміністратора баз даних (в частині КТЗІ);

настанови користувача щодо послуг безпеки;

програма та методика проведення випробувань КТЗІ;

програма навчання користувачів;

програма дослідної експлуатації;

положення про службу захисту інформації;

план захисту інформації;

перелік відомостей, що підлягають захисту;

інструкція по забезпеченню режиму секретності при роботі в ТОВ Альтрон;

інструкція про порядок введення в експлуатацію та модернізацію КТЗІ.

Власником ТОВ Радар розробляються документи:

акт обстеження об’єкта інформаційної діяльності;

паспорт – формуляр;

акти категорування приміщень;

експлуатаційні журнали та інші документи у відповідності до вимог НД ТЗІ та відомчих нормативних документів.

8. Етапи виконання робіт

Таблиця 2.8

Етапи виконання робіт

№ п/п	Назва етапу та робіт по етапу	Термін виконання	Чим закінчується робота
1	Попередній етап	Згідно умов договору	
1.1	Проведення обстеження ОІД		Акт обстеження ОІД
1.2	Визначення переліку загроз і можливих каналів витоку інформації		Модель загроз
1.3	Визначення вимог до КТЗІ в частині захисту від НСД та витоку технічними каналами		Розділи Технічного завдання на створення КСЗІ
2	Етап проектування і розробки КТЗІ	Згідно умов договору	
2.1	Проектування КТЗІ		Вибір проектних рішень
2.2	Розробка техно-робочої та експлуатаційної документації		Проектна та експлуатаційна документація на КТЗІ
2.3	Виконання робіт із захисту інформації від витоку каналами побічних електромагнітних випромінювань та наведень		Протоколи спецдосліджень та приписи на експлуатацію
2.4	Настроювання сервісів безпеки ОС Windows		Виконання настроювань у відповідності до експлуатаційних документів. Протокол приймання робіт
2.5	Розробка організаційної документації та впровадження організаційних заходів захисту		Розроблені і впроваджені організаційні документи та заходи захисту згідно з розділом 5 ТЗ
2.6	Розробка програм та методик випробувань КСЗІ		Програма та методики випробувань
3	Етап випробувань і передачі КТЗІ в експлуатацію	Згідно умов договору	
3.1	Організація та проведення попередніх випробувань КСЗІ		Протоколи попередніх випробувань, акт про приймання КСЗІ в дослідну експлуатацію

Продовження таблиці 2.8

№ п/п	Назва етапу та робіт по етапу	Термін виконання	Чим закінчується робота
3.2	Навчання користувачів		Програма навчання користувачів Акт про завершення навчання
3.3	Організація та проведення дослідної експлуатації КСЗІ		Журнали дослідної експлуатації, акт завершення дослідної експлуатації
3.4	Подача заявки на проведення державної експертизи		Заявка на проведення державної експертизи
4	Державна експертиза КСЗІ	За окремим договором	Атестат відповідності

Підпис Коваленко А.С. _____

Висновок по розділу. При обстеженні об’єкта інформаційної діяльності визначено, що інформація яка буде оброблятись становить державну таємницю. Розроблено згідно вихідних даних, модель можливих загроз та модель вірогідних порушників. На підставі отриманих документів формуємо технічне завдання на побудову КСЗІ. За результатом створення подаємо заявка на експертизу, після схвалення та проведення експертизи отримуємо атестат відповідності.

3 СУЧАСНІ ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1. Системи розмежування доступу до інформації.

Метою розмежування доступу до інформації насамперед є запобігання реалізації загрози порушенням конфіденційності або несанкціонованого доступу до інформації. Можна виділити такі види несанкціонованого доступу:

доступ до носіїв інформації;

локальний доступ до окремих персональних комп'ютерів;

локальний доступ до ресурсів мережі;

віддалений доступ до окремих комп'ютерів або ресурсів мережі.

У перших випадках велике значення мають організаційно-режимні заходи обмеження фізичного доступу до машинним носіям інформації (пропускний режим, охорона, замки на дверях і т.д.). Проте не можна нехтувати і програмно-технічними заходами безпеки.

Щоб відчути всю складність і багатогранність завдання захисту системи від загрози порушення конфіденційності, розглянемо ряд прикладів таких атак. Практично всі вони відносяться до локальних атак, це, однак, не означає, що немає віддалених атак, що дозволяють зловмиснику отримати можливість несанкціонованого доступу до ресурсів системи. Далі буде показано, що атака може бути проведена на будь-якому етапі роботи комп'ютера та користувача у системі.

Соціальна інженерія - Атаки цього не пов'язані безпосередньо з подробицями технічної реалізації інформаційної системи. Основний інструмент таких атак — вплив на персонал та користувачів системи з метою отримання різноманітних інформації на основі психологічних методів з використанням таких людських якостей, як необґрунтована довіра до ненадійно ідентифікованої людини, лінь, неуважність та інших слабкостей. Це не що інше як використання так званого людського фактора. Класичним прикладом такої атаки є ситуація, коли зловмисник

є користувачеві уповноваженою відповідальною особою і змушує його повідомити свій пароль для входу в систему. Безпечність користувачів та їхня зневага до правил інформаційної безпеки безмежні. Паролі вимовляються вголос у присутності незнайомих людей, записуються на папірцях, які потім приклеюються монітору, тощо. У цих випадках дієвими є лише адміністративні заходи, що передбачають суворі (наприклад матеріальні) покарання за відомі випадки розголошення паролів незалежно від наслідків із оповіщенням всіх працівників підприємства.

Потенційно небезпечною є ситуація, коли користувачі та адміністратори мережі змушені через певні причини спілкуватися по телефону. У цьому випадку цілком ймовірним є дзвінок зловмисника адміністратору від імені одного з користувачів з проханням відновити втрачений пароль для входу в систему. Якщо адміністратор не може впевнено ідентифікувати користувача за голосом, така атака може бути успішною.

Особливістю таких атак є абсолютна добровільність (вільна чи мимовільна), з якою користувач ділиться зі зловмисником конфіденційною інформацією, необхідною для входу до системи. Боротися з такими атаками дуже складно, оскільки вони використовують різні слабкості людей і можуть бути націлені на особливості характеру і спонтанні реакції конкретного співробітника підприємства.

Апаратні закладки. - Апаратною закладкою називають пристрій, який виконує недокументовані дії, як правило, на шкоду користувачеві інформаційної системи. Перевірки обладнання на наявність апаратних закладок виробляються лише у системах , що працюють з інформацією підвищеного рівня таємності Більшість користувачів (і фахівців з інформаційної безпеки) навіть не замислюються про можливість існування таких пристроїв, які можуть накопичувати та передавати своєму господарю інформацію про систему та її користувачів.

В даний час користувачі банкоматів мають реальні шанси випробувати роботу таких закладок. Нещодавно в Інтернеті з'явився огляд способів, за допомогою яких зловмисники одержують доступ до даних кредитних карток.

Серед них - використання додаткових зчитувачів магнітних карт, які встановлювалися поверх вхідної щілини штатного зчитувача, та додаткових клавіатур, що реєструють натискання клавіш під час введення пін-коду. З цією ж метою використовувалися мініатюрні відеокамери, що "підглядають" за процесом введення пін-коду. Отримана інформація використовувалася для виготовлення фальшивих кредитних карток та отримання за ними грошей з рахунку потерпілого.

Атака на етапі завантаження. Як відомо, при включенні комп'ютера в його пам'ять завантажується і починає працювати програма, записана в постійному пристрої, призначена для діагностики апаратного забезпечення, зміни налаштувань і завантаження в оперативну пам'ять позасистемного завантажувача. Зазвичай ця програма надає можливість захисту процесу завантаження паролем. Це перша лінія захисту персонального комп'ютера. Якщо не встановлено, зловмисник може, змінивши налаштування, дозволити завантаження зі знімного диска і завантажити комп'ютер, використовуючи носій, що принесений з собою. У цьому випадку він отримає доступ до всіх даних на локальному диску комп'ютера, а в подальшому - до ідентифікаційної інформації користувачів, що працюють на даному ПК. Оскільки сучасні комп'ютери дозволяють проводити завантаження з різних носіїв і фізичних портів, питання про можливість їх використання користувачами стає дуже важливим при визначенні рівня безпеки системи.

Недоліком використання пароля BIOS є можливість скидання при вимкненні батареї на материнській платі. Крім того, алгоритми зберігання паролів BIOS мають ряд істотних недоліків, що полегшують їх підбір, а в деяких випадках виявлено існування універсальних технологічних паролів, встановлених виробником BIOS, що дозволяють отримати доступ до будь-якого ПК, що використовує BIOS цієї фірми.

Атаки на засоби автентифікації. Створення безпечної інформаційної системи неможливе без використання засобів ідентифікації та автентифікації користувачів.

Ідентифікація користувача являє собою порівняння ідентифікатора, що пред'являється користувачем, з наявними в базі раніше виданих системою.

Аутентифікація — перевірка належності цього ідентифікатора користувача. Це автентифікація користувача.

Дуже часто використовується поняття облікового запису, що є об'єднанням ідентифікатора і пароля користувача.

Продовження роботи користувача після завантаження комп'ютера в захищеній системі можливе лише після успішного проходження ним процедур ідентифікації та аутентифікації. Доказом правомірності використання цього ідентифікатора користувача можуть бути різні ознаки. Система може зажадати від користувача:

індивідуальний об'єкт заданого типу (посвідчення, перепустка, магнітну карту тощо), званий токеном;

біометричні характеристики (голосові характеристики,

відбитки пальців, малюнок сітківки ока тощо);

знання інформації (пароль).

Розрізняють пряму аутентифікацію та аутентифікацію за участю третьої сторони. У першому випадку у процесі беруть участь лише дві сторони: користувач та система, ресурсами якої він хоче скористатися. Другий варіант має на увазі участь третьої довіреної сторони. У разі автоматизованої інформаційної системи у цій якості може бути сервер аутентифікації.

Найбільш поширені нині парольні системи. Пароль є відомою лише даному користувачеві послідовністю символів. Способи парольної автентифікації можуть бути різними:

по копії пароля або його згортці, що зберігається в системі;

за деяким перевірочним значенням;

без передачі інформації про паролі стороні, що перевіряє, так званий доказ з нульовим розголошенням.

Ці методи з'явилися в середині 1980 - на початку 1990-х років. Основна ідея методу у тому, що є можливість доказу знання правильного пароля без передачі самого пароля. Після кількох циклів інформаційного обміну сторона із заданою ймовірністю робить висновок про те, що користувачеві пароль відомий;

з використанням пароля для отримання кріптоключа. Основними типами загроз безпеки парольних систем є:

1. Розголошення параметрів облікового запису через:

інтерактивний підбір;

підгляд;

навмисну передачу іншій особі;

захоплення бази даних парольної системи;

перехоплення інформації при передачі по мережі;

зберігання пароля у доступному місці.

2. Втручання у функціонування парольної системи через:

програмні закладки;

використання помилок розробників;

виведення з ладу парольної системи;

типові помилки користувача:

Вибір «легкого» пароля,

Використання доступної стороннім шпаргалки із записаним на ній «складним» паролем,

Введення пароля при сторонніх,

Передача пароля іншій особі.

Способи реалізації цих загроз також можуть бути різними. Виділяють такі можливості для атак:

на пароль у процесі доставки від користувача до місця перевірки в системі;

на спосіб зберігання пароля у системі;

з використанням уразливостей у політиці паролів у системі;

на "слабкі паролі".

Як правило, у сучасних обчислювальних системах використовується аутентифікація користувачів за участю третьої сторони. Всі дані про їхні права в системі зберігаються на виділеному сервері, або навіть на двох. Прикладом таких систем можуть бути широко поширений єдиний каталог Microsoft Active Directory і єдиний каталог мережевої операційної системи Novell Netware. У цьому випадку

інформація про введений користувачем пароль передається в систему аутентифікації по мережі одним з наступних способів:

відкритим. Так працюють відомі протоколи Telnet та FTP

після шифрування;

у вигляді згортки зі спеціальною хеш-функцією (хешування);

без безпосередньої передачі інформації про пароль.

Тому при створенні моделі інформаційної безпеки необхідно враховувати можливість перехоплення зловмисником пароля користувача, що передається по мережі. Той факт, що уряд США зняв обмеження на експорт сильних криптографічних систем, може означати, що в його (і, можливо, не тільки в його) розпорядженні нині знаходяться обчислювальні потужності, що дозволяють зламувати широко розповсюджений протокол шифрування SSL із довжиною ключа 128 біт. за розумний проміжок часу. Таким чином, не можна говорити про повну безпеку таких систем.

Особливу увагу розробники приділяють способам зберігання паролів. Найчастіше використовуються такі:

у відкритому вигляді;

у вигляді згортки;

у зашифрованому вигляді.

Спосіб зберігання паролів у системі змінити неможливо, тому необхідно дуже ретельно простежити всі відгалуження інформаційних потоків, пов'язані з паролі, що містять файли або бази даних. У багатьох системах задля забезпечення відмови стійкості створюється резервна копія цих даних. Якщо зловмисник зможе отримати у своєму розпорядженні файл з паролями або його копію, він матиме достатньо часу, щоб спробувати його проаналізувати та отримати додаткову інформацію, яку можна використовувати при зломі системи.

Політика паролів зазвичай пропонує широкий набір засобів, основною метою яких є утруднення роботи парольного зломщика — програми підбору пароля за тими чи іншими алгоритмами. Вона включає установку мінімального часу очікування між послідовними спробами входу, обмеження за кількістю спроб

входу в систему з подальшим блокуванням облікового запису користувача і посилкою повідомлення адміністратору системи або адміністратору безпеки. Велика увага приділяється роботі з користувачем. Можна встановити автоматичні обмеження на мінімальну довжину пароля та обов'язковість зміни пароля через певний проміжок часу. При цьому використані раніше вказаним користувачем паролі зберігаються в базі даних, і система стежить за тим, щоб він використовував щоразу нові паролі. Можна визначити мінімальну якість пароля, змусивши користувача застосовувати при зміні пароля символи на різних регістрах і спецсимволи, відбраковувати паролі, що легко підбираються. Недоліком застосування дуже суворої політики може бути складність запам'ятовування невимовних паролів користувачами, оскільки будь-яке осмислене поєднання букв у цьому випадку автоматично вважається слабким паролем. В результаті паролі записуватимуться на папірцях і наклеюватимуться на монітор, що, очевидно, зведе нанівець усі заходи безпеки. У цьому випадку особливу важливість набувають адміністративні заходи з боку керівництва.

Однією з цілей застосування політики паролів є боротьба з так званими слабкими паролями. Як правило, користувачі, будучи наданими самі собі, не дуже утрудняються при виборі пароля входу в систему. Найчастіше як пароль вибирають рік народження, власне ім'я або прізвище, телефон (робочий або домашній), ім'я коханої людини, кличку собаки тощо. Верхом секретності в цьому випадку буде введення російського слова з використанням англійської розкладки клавіатури або заміна деяких літер подібними до накреслення спецсимволами. Всі ці особливості людської психіки давно враховані творцями спеціальних програм для підбору паролів парольних зломщиків. Відомо, що прямий перебір комбінацій при підборі досить довгого пароля, створеного на базі великого алфавіту, який у випадку комп'ютерної клавіатури включає літери всіх використовуваних на од ній машині розкладок клавіатури та спецсимволи, є тривалою процедурою. Тому більшість парольних зломників працюють зі словниками типових паролів, що часто використовуються, враховуючи особливості мовного середовища, менталітету та інших особливостей атакованого користувача. Цей спосіб у поєднанні з

попередньою розвідкою дає непогані результати, якщо в організації не використовуються програми - генератори хороших паролів.

Класичною атакою на парольну систему є фальшування запрошення введення імені та пароля при вході в систему. Цього можна досягти шляхом впровадження (найчастіше методами соціальної інженерії) у комп'ютер користувача спеціального програмного забезпечення, що імітує діалог, що запрошує ввести ім'я та пароль, що відповідають встановленій на комп'ютері операційній системі. Якщо користувач буде недостатньо уважний до деталей поведінки системи та зовнішнього вигляду вікна – запрошення, він не зможе відрізнити підробку, і його ідентифікаційна інформація може стати відома зловмиснику. Необхідно звертати увагу на послідовність, кількість запитів та інтервали між ними, форму та колірне рішення діалогів тощо. Якщо мають місце якісь зміни у звичній процедурі, велика ймовірність того, що ви стали об'єктом атаки. Можливо, успішною.

Як зазначалося вище, токеном називають пристрій, що містить унікальний параметр. Пропуск на паперовому носії можна також назвати токеном, лише інформація, що міститься в ньому, зчитується і обробляється співробітником охорони. У найпростішому випадку при підключенні токена до системи остання зчитує значення ключового параметра і порівнює його з тим зразком, що зберігається в базі даних (див. вище способи зберігання паролів). При збігу, користувач може продовжити роботу в системі. Можливі інші способи реалізації роботи з токеном.

Якщо система та токен мають однакові синхронізовані системи генерування одноразових паролів, то при підключенні токена стартують процеси генерації в системі та в токені. Якщо результати збігаються, користувач отримує доступ до роботи. Існують інші, більш складні способи роботи з токеном, що використовують криптографічні методи типу електронного підпису або потребують додаткової автентифікації користувача шляхом введення так званого пін-коду.

Внутрішні механізми роботи токена приховані від користувача, і найчастіше не повинен запам'ятовувати жодної додаткової інформації для отримання доступу до системи. Це зручно, але виникає потреба протягом робочого часу мати токен при собі. На щастя, сучасні технології дозволяють виготовляти токени у вигляді компактних пристроїв розміром не більше брелока для ключів.

Атаки на використовуючі токени системи базуються на індивідуальних особливостях алгоритмів обміну інформацією, що працюють у них. Наприклад, при передачі параметра по мережі, що міститься в токені, існує ймовірність його перехоплення. Однак, малі розміри та вага токенів роблять куди більш ймовірними їхню втрату або розкрадання.

Використання біометричних характеристик людини для аутентифікації вважається нині дуже перспективним напрямом. Біометричні ознаки - це теж свого роду токен, що природно присутній в організмі людини. Такі системи аутентифікації характеризуються такими параметрами:

Рівень хибної відмови. Це відсоток відмов у доступі при пред'явленні свідомо коректного автентифікатора.

Рівень хибного підтвердження. Це відсоток ухвалення некоректного автентифікатора.

Швидкість обробки автентифікатора.

Стійкість до заміни.

Вимоги щодо зберігання даних.

Додаткові умови.

Необхідно відзначити, що завдання використання біометричних параметрів при аутентифікації дуже складне з алгоритмічної точки зору і вимагає значних ресурсів для зберігання та обробки аутентифікаційних даних, оскільки останні найчастіше є зображення або багатовимірні вектори. Крім того, користувачі висувають дуже жорсткі вимоги до швидкості обробки автентифікаційної інформації. Додаткові проблеми можуть виникнути через культурні або фізіологічні особливості користувачів. Наприклад, дотик багатьох людей до того

самого пристрою може виявитися неприйнятним для людей з іншими культурними традиціями.

Атаки на системи з аутентифікацією за біометричними параметрами фактично зводяться до атак (іноді фізичних) на їх авторизованих користувачів та спроб перехоплення аутентифікаційної інформації, що передається по мережі.

При створенні моделі інформаційної безпеки необхідно враховувати, що, отримавши доступ до системи, користувач (а можливо і зловмисник, який зумів проникнути в систему від імені даного користувача) може виконувати різні несанкціоновані дії. Прикладом таких дій може бути пошук додаткової інформації в системі, наприклад, шляхом аналізу системного «сміття» або спроби доступу до баз даних поза системою розмежування прав, не використовуючи штатні програми. Таким чином, він може отримати доступ до інформації, яка для нього не призначена. Такі атаки називаються «підвищенням прав».

Значно великі можливості для підвищення прав дає несанкціонована установка користувачем на своєму комп'ютері стороннього програмного забезпечення. Це може бути зроблено неусвідомлено в ході віддаленої атаки на його комп'ютер або усвідомлено для дослідження та злому системи (якщо діє зловмисник або просто надмірно цікавий співробітник). Прикладами таких програм можуть бути:

програми підвищення прав користувача;

сніффери;

програми підбору паролів;

зломники шифрів;

дизассемблери;

програми створення вірусів;

конструктори та генератори мережевих пакетів;

програми автоматичного пошуку вразливостей операційної системи.

Роздивимось одну із систем на прикладі:

ГРИФ-ХР ВЕРСІЙ 1.ХХ.

Комплекс засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу 1. Реалізуємий функціональний профіль КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1,ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 з рівнем гарантій Г-4.

Комплекс засобів захисту (КЗЗ) інформації "Гриф-ХР" призначений для забезпечення захисту інформації з обмеженим доступом (ІзОД), у тому числі інформації, що становить державну таємницю, конфіденційної інформації, яка є власністю держави, інформації, що становить комерційну таємницю, при її обробці в автоматизованих системах класу "1" на базі персональних комп'ютерів під управлінням операційної системи (ОС) MS Windows XP Professional. Комплекс дозволяє створити на базі персонального комп'ютера спеціалізоване робоче місце з обмеженим кругом користувачів і забезпечити захист оброблюваної ІзОД від загроз цілісності, конфіденційності і доступності при реалізації політики адміністративного управління доступом до інформації, тобто захистити інформацію від несанкціонованого ознайомлення, модифікації, видалення.

Комплекс «Гриф-ХР» реалізує наступні функції:

ідентифікацію і автентифікацію користувачів на підставі імені, пароля і носія даних автентифікації (дискети, Flash, інших змінних дисків або Touch Memory), що дозволяє розпізнати авторизованого користувача і надалі реагувати на запити цього користувача відповідно до його повноважень;

блокування завантаження ОС із змінних носіїв (ця функція реалізується апаратною компонентою, яка поставляється опційно) що дозволяє заблокувати завантаження ОС і використання ПЕОМ сторонньою особою, а також гарантувати включення в роботу усіх компонентів КСЗ;

розмежування обов'язків користувачів і виділення декількох ролей адміністраторів, які можуть виконувати різні функції по адмініструванню (реєстрацію ресурсів, що захищаються, реєстрацію користувачів, призначення прав доступу, обробку протоколів аудиту і тому подібне);

розмежування доступу користувачів до каталогів (текам) відповідно до принципів адміністративного управління доступом, що дозволяє організувати

спільну роботу на ПЕОМ декількох користувачів, що мають різні службові обов'язки і права по доступу до ІзОД;

управління потоками інформації і блокування потоків інформації, що призводять до зниження її конфіденційності (наприклад, при за рахунок копіювання файлів або перенесення інформації через системний буфер обміну); контроль за виводом інформації на друк;

контроль за експортом інформації на змінні носії і її імпортом;

гарантоване видалення інформації шляхом затирання вмісту файлів, ІзОД;

розмежування доступу прикладних програм до захищених каталогів, що дозволяє забезпечити захист ІзОД від несанкціонованого або випадкового видалення, модифікації і дотримати технологію її обробки;

контроль цілісності прикладного програмного забезпечення і ПЗ КЗЗ а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотримання технології обробки ІзОД; контроль за використанням дискового простору користувачами (квоти), що виключає можливість блокування одним із користувачів роботи інших;

можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

контроль цілісності і само тестування КЗЗ при старті;

відновлення функціонування КСЗ після збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї;

реєстрацію подій (входу користувача в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з ІзОД, виводу на друк і так далі) в спеціальних протоколах аудиту що дозволяє адміністраторам контролювати доступ до інформації, стежити за тим, як використовується КСЗ, а також правильно його конфігурувати

3.2. Антивіврусні засоби

Avast! Free Antivirus — Безкоштовний антивірус Avast є основним продуктом у лінійці. Існують додаткові версії, які додають більше функцій, але не є безкоштовними. Крім того, Avast One — це нова версія Avast, яка пропонує більше функцій, ніж безкоштовний антивірус Avast, а також є безкоштовна версія. Ось що постачається з кожною версією Avast:

Безкоштовний антивірус Avast:

Антивірусний захист на основі сигнатур і поведінки

Захист від зловмисного програмного забезпечення, який стежить за активністю підозрілого програмного забезпечення та захищає від відомих або підозрілих веб-сайтів

Захист від програм-вимагачів, який ідентифікує програму-вимагач за поведінкою, запобігаючи змінам файлів і запобігаючи запуску програм-вимагачів

Перевіряє на наявність порушень пароля

Захист Wi-Fi, що включає пробну версію бездротового VPN

Захист мережі для домашнього WiFi

Блокування перерв для презентацій, фільмів та інших заходів

CyberCapture, який надсилає підозріле програмне забезпечення в хмару для аналізу, а потім створює виправлення для надсилання всім користувачам

Smart Scan для перевірки проблемних налаштувань, застарілого програмного забезпечення та налаштувань

Захист електронної пошти для підтримуваних поштових клієнтів запобігає отриманню зловмисного програмного забезпечення через з’єднання електронної поштиінструменти для очищення браузерів від плагінів з поганою репутацію. Плагін для повідомлення про репутацію веб-сайтів (Мал.3.1.).

Мал. 3.1. Вікно Avast! Free Antivirus

Avira Free Antivirus — Avira має популярне безплатне антивірусне програмне забезпечення, яке включає ряд додаткових утиліт і три різні платні варіанти, кожен з яких має гарантію повернення грошей:

Безплатна версія Avira — це набір програмного забезпечення, який включає антивірусний захист, захист від програм-вимагачів тощо. Він доступний для Windows, Mac, Android та iOS:

Повне сканування системи на віруси та шкідливі програми

Карантин підозрілих файлів або файлів із високим ризиком

Брандмауер для блокування онлайн-атак

Захист від програм-вимагачів

Оновлено програмне забезпечення, щоб ваші програми мали найновіші виправлення безпеки

Блокування трекерів браузера для припинення реклами та завантаження небажаного програмного забезпечення

VPN для анонімного перегляду

Менеджер паролів, який генерує та зберігає облікові дані для входу

Оптимізатор запуску та очищувач дискового простору

Можливість роботи за розкладом (Мал. 3.2.).

Мал. 3.2. Вікно Avira Free Antivirus

AVG AntiVirus Free — AVG пропонує три рівні антивірусного захисту для Windows. Пакети починаються з AVG Antivirus Free, який пропонує хороший захист для безплатного продукту. Існує також антивірусне програмне забезпечення для комп'ютерів MacOS і мобільних пристроїв Android. Крім того, AVG пропонує програмне забезпечення безпеки у вигляді VPN та програмного забезпечення для захисту від відстеження для комп'ютерів Windows і Macintosh, а також пристроїв Android та iOS.

Безплатний антивірус AVG:

Зупиняє віруси та шкідливі програми

Захист від зловмисного програмного забезпечення, який стежить за активністю підозрілого програмного забезпечення та захищає від відомих або підозрілих вебсайт

Захист від програм-вимагачів, який ідентифікує програму-вимагач за поведінкою, запобігаючи змінам файлів і запобігаючи запуску програм-вимагачів

Блокування перерв для презентацій, фільмів та інших заходів

Відправляє підозріле програмне забезпечення в хмару для аналізу, а потім створює виправлення для надсилання всім користувачам

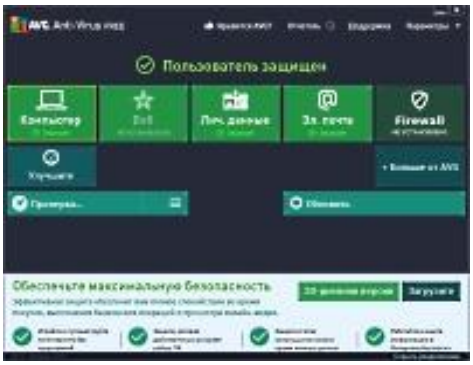
Smart Scan для перевірки проблемних налаштувань, застарілого програмного забезпечення та налаштувань

Захист електронної пошти для підтримуваних поштових клієнтів запобігає отриманню зловмисного програмного забезпечення через з'єднання електронної пошти

WiFi Inspector забезпечує виявлення вторгнень.

Також доступно для комп'ютерів Macintosh

Мале споживання системних ресурсів (Мал. 3.3.).



Мал. 3.3. Вікно AVG AntiVirus Free

Panda Free Antivirus — перший безкоштовний, «хмарний» антивірус, робота якого базована на принципі захисту «з хмари» в режимі реального часу. Ця програма об'єднує локальний і віддалений антивірус, антишпигун, антіруткит, евристичну перевірку і кешування нешкідливого програмного забезпечення (*goodware*).

Нова «хмарна» модель антивіруса використовує надлегкий «тонкий клієнт» локально встановлений на комп'ютері, що зв'язаний з серверами Panda. Такий принцип, у порівнянні з локально встановленим антивірусом (базованим на сигнатурному принципі захисту), дозволяє ефективніше здійснювати виявлення

і блокування шкідливих програм. «Тонкий клієнт» Panda Free Antivirus використовує сучасні «надлегкі» технології перехоплення шкідливих програм. Таким чином використовується на 50% менше ресурсів комп'ютера у порівнянні з традиційним антивірусом.

Основні характеристики Panda Free Antivirus:

поведінковий екран. Захист від дій, які, як правило, виконуються шкідливими програмами;

вбудований захист від дроперів PDF, DOC, XLS, PPT, WMV і т. д.;

можливість увімкнення/вимкнення й налаштування поведінки різних систем, відповідей «хмари», розширеного протоколювання, налаштування кошика, виключень і т.д.;

самозахист процесів антивіруса і його конфігурацій;

можливість запуску разом з іншими програмами захисту системи;

багатомовна підтримка;

режим роботи у реальному часі;

використовує мінімум ресурсів (всього 17 MB оперативної пам'яті);

ефективне виявлення і блокування шкідливих програм;

не отримує щоденних оновлень, а використовує онлайн-базу даних (Мал. 3.4.).

Мал. 3.4. Вікно Panda Free Antivirus

Zillya! — безкоштовний антивірус що пропонує захист від будь-якого типу загроз: вірусів, червів, троянів, руткітів, і інших шкідливих програм, діяльність яких призводить до некоректної роботи системи, втрати або пошкодження даних. Також Zillya! виявляє шпигунські і рекламні програми, ефективно блокує і видаляє їх, захищаючи тим самим користувача від агресивної реклами і проникнення сторонніх осіб до особистої інформації. Антивірус Zillya! має три режими сканування (швидке, повне і власне), а також можливість запуску сканування за розкладом в потрібний для користувача час. Кожен режим сканування виконується з певними параметрами відповідно до призначення режиму. Швидке сканування — експрес-перевірка найуразливіших областей системи. Повне сканування — ретельна перевірка системи. Власне сканування — сканування з налаштуваннями користувача.

Основні характеристики Zillya!:

ефективний захист від будь-якого типу загроз;

вибір режимів сканування та сканування за розкладом;

вбудований алгоритм евристичного аналізу;

виявляє шпигунські і рекламні програми шкідливого характеру;

сканує поштові повідомлення (вхідні і вихідні) і вкладені в них файли;

сканує документи перед їх відкриттям;

сканує файли, завантажені з Інтернету;

перевірка в режимі реального часу;

перевірка з налаштуваннями користувача (Мал. 3.5.).

Мал. 3.5. Вікно Zillya.

Антивірус Kaspersky Free — «Лабораторія Касперського» вже більше ніж двоє десятиліть має високу оцінку охоронної компанії. Він отримав хороші оцінки від професійних рецензентів за свої інтуїтивно зрозумілі антивірусні продукти та надійне виявлення шкідливих програм, яким допомагає машинне навчання. Kaspersky продає своє програмне забезпечення в більш ніж 200 країнах і має 35 офісів у 31 країні. У ньому працює команда з 4000 спеціалістів з безпеки.

Простий інтерфейс «Лабораторії Касперського» робить її хорошим вибором для нетехнічних користувачів, які отримують сповіщення та можуть просто клацнути, щоб видалити підозрілі файли. Він пропонує чотири різні пакети для домашніх користувачів, від базового Антивірусу Касперського до пакета Security Cloud Personal, зі знижками на перший рік до 50%. Залежно від ваших уподобань та бюджету, ви можете отримати пакети з додатковими інструментами конфіденційності, включаючи віртуальну приватну мережу (VPN), блокувальник реклами та блокувальник вмісту для дорослих. У преміумклас Kaspersky Security Cloud є всі ці параметри та додається «перевірка облікового запису», щоб повідомити вас, якщо ваші облікові записи Netflix, Facebook чи інші були зламані. Пакет преміумклас також пропонує поради щодо того, як керувати порушеннями, і включає функції, спрямовані на забезпечення безпеки дітей в Інтернеті та офлайн, включаючи фільтрацію YouTube і вебсайт, моніторинг часу використання екрана та GPS-відстеження.

Ad-Aware Free Antivirus+ — Adaware Antivirus Free (раніше Ad-Aware Free Antivirus+) – безплатний антивірус, що використовує технології Bitdefender, легендарний антишпигун Ad-Aware для виявлення та блокування всіх видів шкідливих програм та онлайн-загроз.

Якщо озирнутися в минуле досить далеко, то можна знайти антивірусне програмне забезпечення, яке суворо спрямоване на захист від комп’ютерних вірусів, оскільки

інші види шкідливого програмного забезпечення були в кращому випадку рідкістю. Оскільки проблеми рекламного та шпигунського програмного забезпечення з’явилися, деякі компанії безпеки зосередилися на них. Це було походженням Ad-Aware. Як і практично всі сучасні антивірусні продукти, поточний Adaware Antivirus Free має на меті знищити всі типи шкідливих програм.

Більшість антивірусних продуктів отримують оновлений огляд із новим випуском щороку або близько того. Adaware — принаймні, не останнім часом. Його веб-сайт, здається, застряг у 2017 році. Однак, за спостереженнями, його визначення сигнатур зловмисного програмного забезпечення є абсолютно актуальними, а це найважливіше для такого продукту. У платних версіях Adaware використовуються передові методи, включаючи виявлення на основі поведінки, але безкоштовна версія спирається на просте розпізнавання шаблонів..

ВИСНОВКИ

Питання захисту інформації в інформаційно-телекомунікаційних системах дуже актуальне на даний час.

На основі аналізу нормативних документів встановлені вимоги до захисту конфіденційної та таємної інформації.

Проаналізовано існуючі загрози інформації в інформаційно-телекомунікаційних системах. Встановлено, що існують загрози витоку технічними каналами, та загрози несанкціонованих дій з інформацією.

Для захисту інформації від витоку технічними каналами використовуються апаратні засоби. Для захисту інформації від несанкціонованих дій застосовуються програмні засоби.

В рамках роботи проведено обстеження середовищ функціонування інформаційно-телекомунікаційної системи, розроблені моделі загроз інформаційній безпеки та порушника, політика інформаційної безпеки, технічне завдання.

Проаналізовано сучасні програмні засоби захисту інформації в АС 1.

Для захисту інформації в АС класу 1 застосовано комплекс засобів захисту Гриф 3 та вітчизняний антивірус Zillya.

Таким чином мета роботи досягнута.

ПЕРЕЛІК ПОСИЛАНЬ

Законодавчі та нормативні документи

1. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

3. Закон України «Про Національну систему конфіденційного зв'язку»

4. Закон України «Про інформацію»

5. Закон України «Про телекомунікації»

6. Закон України «Про радіочастотний ресурс України»

7. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»

8. Закон України «Про державну таємницю»

9. Закон України «Про ліцензування певних видів господарської діяльності»

10. Закон України «Про електронні документи та електронний документообіг»

11. Закон України «Про наукову і науково-технічну експертизу»

12. Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання»

13. Закон України «Про ратифікацію Статуту і Конвенції міжнародного союзу електрозв’язку»

14. Закон України «Про електронний цифровий підпис», від 22.05.2003 № 852-IV»

15. Закон України «Про електроні документи та електронний документообіг», від 22.05.2003 № 851-IV»

16. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної

системи захисту інформації в інформаційно-телекомунікаційній системі.

17. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

18. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

19. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

20. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

22. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 №

23. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

Електронні ресурси

24. Правові основи діяльності Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" від 15 березня 2016 року № 96/2016"www.dstszi.gov.ua

25. Нормативна правова база Держспецзв'язку, закони http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/