Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования

Национальный исследовательский университет “МИЭТ”

Институт Системной и программной инженерии и информационных технологий

## Практическое занятие 2

**Дисциплина: Информационная безопасность**

Выполнили студенты П-32:

Селезнева Валерия  
Утева Александра

Москва, 2021

УТВЕРЖДАЮ

Генеральный директор

ООО «Ромашка»

ФИО

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_2021г.

Модель угроз и нарушителя

безопасности информации объекта АС

«Pharmacy»

ООО «Ромашка»

(ПРОЕКТ)

Москва, 2021

# Общие положения

Настоящий документ содержит актуальные угрозы безопасности информации автоматизированной системы «Pharmacy» ООО «Ромашка» (далее – АС «Pharmacy») категории АС 2Б (СВТ КЗ 5), которые должны быть заблокированы (нейтрализованы) путем принятия организационно-технических и режимных мер по защите информации. Настоящий документ разработан с учётом положений модели угроз и нарушителя безопасности информации ООО «Ромашка».

В настоящем документе приведены оценка возможностей (потенциала) нарушителей безопасности информации, анализ возможных уязвимостей и способов реализации угроз безопасности информации, и последствий от нарушения свойств безопасности информации, обрабатываемой в АС.

В документе учтены результаты проведённого обследования АС, а также особенности структурно-функциональных характеристик АС «Pharmacy».

# Назначение и область действия документа

Настоящий документ предназначен для определения и оценки угроз безопасности информации объект АС, а также разработки организационно- технических и режимных мер по защите информации, обеспечивающих нейтрализацию предполагаемых угроз.

**В разделе 1** «Общие положения» приведены:

* назначение и область действия документа;
* нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз;
* наименование обладателя информации, заказчика, оператора систем и сетей;
* подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей;
* наименование организации, привлекаемой для разработки модели угроз безопасности информации.

**В разделе 2** «Описание систем и сетей и их характеристика как объектов защиты» приведены:

* наименование систем и сетей, для которых разработана модель угроз безопасности информации;
* класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных;
* нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети;
* назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим;
* основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети;
* состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;
* описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется;
* описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;
* информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления вычислительных услуг, о распределении ответственности за защиту информации между обладателем информации, оператором и поставщиком вычислительных услуг, об условиях использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг.

**В разделе 3** «Возможные негативные последствия от реализации (возникновения) угроз безопасности информации» приведены:

* описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов;
* описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба).

**В разделе 4** «Возможные объекты воздействия угроз безопасности информации» приведены:

* наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемой информации, или обеспечивают реализацию основных процессов обладателя информации, оператора;
* описание видов воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям.

**В разделе 5** «Источники угроз безопасности информации» приведены:

* характеристика нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации;
* категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации;
* описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

**В разделе 6** «Способы реализации (возникновения) угроз безопасности информации» приведены:

* описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы нарушителями разных видов и категорий;
* описание интерфейсов объектов воздействия, доступных для использования нарушителями способов реализации угроз безопасности информации.

**В разделе 7** «Актуальные угрозы безопасности информации» приведены:

* перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей;
* описание возможных сценариев реализации угроз безопасности информации;
* выводы об актуальности угроз безопасности информации.

В «Приложении А» приводятся схемы и рисунки, иллюстрирующие состав, архитектура систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы.

В «Приложении Б» приводятся схемы с отображением объектов воздействия и их назначения в составе архитектуры систем и сетей.

В «Приложении В» приводятся рисунки, иллюстрирующие возможности нарушителей, и другие поясняющие материалы.

В «Приложении Г» приводятся схемы с отображением типов логических, физических интерфейсов объектов воздействия, в том числе требующих физического доступа к ним, а также соответствующие им способы реализации угроз безопасности информации.

В «Приложении Д» приводятся схемы с отображением сценариев реализации угроз безопасности информации.

# Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз

При разработке настоящего документа учитывались действующее законодательство, нормативные правовые акты и методические документы уполномоченных федеральных органов исполнительной власти, в которых регламентируются вопросы разработки моделей угроз безопасности информации, применимые положения национальных стандартов и иных документов (источников), в том числе:

* Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
* Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
* Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* нормативный правовой акт ФСТЭК России «Требования о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах», утвержден приказом ФСТЭК России от 11.02.2013 № 17;
* нормативный правовой акт ФСТЭК России «Состав и содержание организационных н технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержден приказом ФСТЭК России от 18.02.2013 № 21;
* нормативный правовой акт ФСТЭК России «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционированиям, утвержденный приказом ФСГЭК России от 21.12.2017 № 235;
* нормативный правовой акт ФСТЭК России «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденный приказом ФСТЭК России от 25.12.2017 № 239;
* методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014;
* «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утверждена приказом ФАПСИ от 13.06.2001 № 152;
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждены приказом ФСБ России от 10.07.2014 № 378;
* «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утверждены руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432;
* «Методика оценки угроз безопасности информации», утверждена ФСТЭК России 05.02.2021;
* банк данных угроз безопасности информации ФСТЭК России.

А также локальные нормативные акты ООО «Ромашка»:

* Политика информационной безопасности ООО «Ромашка», утвержденная приказом от 28.10.2020
* Политика ООО «Ромашка» в области обработки и обеспечения безопасности персональных данных, утверждена приказом № 2020Д от 20.03.2020
* Концепция построения системы информационной безопасности, утвержденная приказом от 29.11.2020;
* А.01.00.2020, утверждено приказом № 582ОД(а) от 26.07.2020
* 10.01-90-2020 Положение об информационно-новостных ресурсах ООО «Ромашка», утверждено приказом № 25ИНР от 06.11.2020
* 10.01-2020 Положение о порядке организации совещаний в ООО «Ромашка», утверждено приказом № 23ПОС от 26.06.2020
* 11-015 Положение о порядке проведения переговоров с потенциальными заказчиками, утверждено приказом № 22ПППсПЗ от 10.06.2020
* 20-2020 Положение о порядке применения паролей доступа для обеспечения информационной безопасности ООО «Ромашка», утверждено приказом № 24 от 21.04.2014
* 0-24-2020 Положение о прядке безопасности использования внешней электронной почты в ООО «Ромашка», утверждено приказом № 26 от 21.04.2020
* 0-27-2020 «Положение о порядке безопасного использования ресурсов сети Интернет в ООО «Ромашка», утверждено приказом № 278 от 21.04.2020
* 0-27-2020 «Положение о порядке антивирусной защиты в ООО «Ромашка», утверждено приказом № 228 от 01.11.2020
* 14 Положение «Порядок обеспечения эксплуатации и обслуживания средств вычислительной техники и программного обеспечения», утверждено приказом № 227 от 15.10.2020
* .1144-2020 Положение процедура управления информационными активами в ООО «Ромашка», утверждено приказом № 225 от 06.06.2020
* .1145-2016 Внедрение и эксплуатация информационных систем в ООО «Ромашка», утверждено приказом № 222 от 06.06.2016
* 27.1014-2016 «Положение о коммерческой тайне ООО «Ромашка», утверждено приказом № 221 от 29.06.2020
* -2020 Положение об управлении доступом к ресурсам корпоративной сети ООО «Ромашка», утверждено приказом № 220 от 27.08.2020
* -2020 Положение об аудите информационной безопасности, утверждено приказом № 219 от 25.03.2020
* 2020 Положение о безопасном использовании съемных носителей информации в ООО «Ромашка», утверждено приказом № 218 от 26.06.2020
* 1143-2016 Положение. Безопасное использование мобильных средств вычислительной техники, утверждено приказом № 215 от 16.06.2020
* -2020 Безопасность сетевой инфраструктуры в ООО «Ромашка», утверждено приказом № 213 от 15.02.2020
* 1194-2020 Управление рисками информационной безопасности ООО «Ромашка», утверждено приказом № 210 от 24.11.2020
* .1238-2020 Положение. Административно – управленческие вопросы, система управления. Обучение работников в целях повышения осведомленности в области информационной безопасности в ООО «Ромашка», утверждено приказом № 201 от 03.07.2018
* .00.1239 Положение. Административно – управленческие вопросы, система управления. Управление инцидентами информационной безопасности. Порядок реагирования и устранения, утверждено приказом № 669 от 09.07.2020
* .3084 Административно – управленческие вопросы. Правила, особенности и порядок работы с конфиденциальной информацией, утверждены приказом № 669 от 09.07.2020
* .3274-2019 Положение. Информационные технологии. Управление изменениями информационных систем
* Положение о порядке работы с соглашениями о конфиденциальности, утверждено приказом № 183 ОД от 05.06.2020
* -2020 Регламент «Порядок установки обновлений СУБД и ППО в ООО «Ромашка», утвержден приказом № 300 от 30.03.2020
* -2020 Регламент «Процедура управления изменениями в сетевой инфраструктуре», утвержден приказом № 301 от 11.04.2020
* Регламент управления уязвимостями информационных систем в ООО «Ромашка», утвержден приказом № 302 от 18.12.2020
* Регламент резервного копирования, утвержден приказом № 303 от 27.11.2020
* .4048-2018 Инструкция работника по правилам безопасного хранения электронных документов в ООО «Ромашка», утверждена приказом № 304 от 24.12.2020
* Инструкция по обеспечению безопасности эксплуатации СКЗИ, утверждена приказом № 305 от 16.01.2020
* Инструкция о пропускном и внутриобъектовом режимах в ООО «Ромашка», утверждена приказом № 305 от 28.04.2020
* Перечень сведений конфиденциального характера ООО «Ромашка», утвержден приказом № 345 ОД от 03.04.2020
* Цели в области информационной безопасности ООО «Ромашка», утверждены приказом № 305 ОД от 04.04.2020
* Приказ № 306 от 22.04.2020 «О хранении электронных и производственных данных»;
* Приказ № 307 от 10.04.2020 «Об организации обмена конфиденциальной документации с филиалами»;
* Приказ № 308 от 07.09.2020 «О передаче служебной информации по открытым каналам связи»
* Приказ № 309 от 25.06.2020 «Об использовании электронной почты, сети интернет и электронных носителей»
* Приказ № 310 от 28.12.2020 «О пересылке конфиденциальной информации»
* Приказ № 311 от 13.12.2020 «О внедрении стандарта по обеспечению информационной безопасности»
* Приказ № 312 от 12.12.2020 «О защите информации»

# Наименование обладателя информации, заказчика, оператора систем и сетей

Заказчиком и обладателем информации является ООО «Ромашка».

# Наименование организации, привлекаемой для разработки модели угроз безопасности информации

Модель угроз безопасности информации ООО «Ромашка» разработана с привлечением АО «ЭЛВИС-ПЛЮС», имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации (рег. № 0017 от 01.10.2002).

# Описание систем и сетей и их характеристика как объектов защиты

# Описание системы ООО «Ромашка»

АС «Pharmacy» создана и функционирует в соответствие с приказом № 282 от 01.01.2020 «О вводе в эксплуатацию», утвержденного генеральным директором ООО «Ромашка».

АС «Pharmacy» размещается в пределах контролируемой зоны ООО «Ромашка» по адресу Российская федерация, г. Клин, р-н Клинский, 8 и предназначена для учета лекарственных препаратов. В ней обрабатывается общедоступная информация и информация конфиденциального характера, в соответствие с Перечнем сведений конфиденциального характера ООО «Ромашка», утвержден приказом № 551 от 03.04.2020, информация, циркулирующая в АС «Pharmacy», отнесена к общедоступной, служебной информации.

АС «Pharmacy» создается/функционирует для обеспечения следующих основных процессов (бизнес-процессов) ООО «Ромашка»:

* Видеть список препаратов в наличии/нет в наличии;
* Производить скидку на определённую категорию препаратов;
* Учета препаратов;

В соответствие с:

Актом классификации № 999 от 01.03.2021 в АС «Pharmacy» присвоен класс защищенности 2Б;

Актом определения уровня защищенности ПДн № 1001 от 01.03.2021 АС «Pharmacy» присвоен уровень защищенности 5.

## Состав в АС «Pharmacy»

Состав технических средств (далее – ТС) в АС «Pharmacy» приведен в таблице 1, перечень программного обеспечения (далее – ПО) приведен в таблице 2.

Таблица 1 – Состав ТС в АС «Pharmacy»

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Примечание** |
| 1 | Компьютер | 1 шт. Для взаимодействия с АС и хранения конфиденциальной информации |

Таблица 2 –Перечень ПО АС «Pharmacy»

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Примечание** |
| 1 | 1С:Предприятие 8.Аптека | Для автоматизации деятельности на предприятии |
| 2 | Операционная система Windows 10 | Для управления с помощью графического интерфейса |
| 3 | Антивирус “Касперский” | Для защиты от вирусов, троянов, шпионских программ |

## Описание пользователей АС «Pharmacy»

### Внешние пользователи

Отсутствуют внешние пользователи

### Внутренние пользователи

Все внутренние пользователи наделены равными полномочиями:

Просмотр, добавление, изменение и удаление карточек с информацией о препаратах;

## Описание внешних интерфейсов и взаимодействий систем и сетей с пользователями

Внешние интерфейсы отсутствуют, так как АС не предоставляет доступа в интернет

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| **Устройство** | **Имя устройства** | **Интерфейс** | **IP адрес/маска** |

В связи с отсутствием сведений по обеспечению безопасности информации со стороны оператора услуг связи, принимается, что за пределами ИР ООО «Ромашка» находится скомпрометированные ресурсы, на которых злоумышленник обладает всеми возможностями для воздействия на информацию.

Учет машинных носителей информации осуществляется \_\_\_\_\_\_. Контроль использования внешних носителей информации осуществляется через программное обеспечение Антивирус Касперского. У пользователей имеется возможность использовать машинные носители информации на всех АС ОКИИ.

Неиспользованные порты на сетевом оборудовании не опечатаны.

Схемы и рисунки, иллюстрирующие состав и архитектуру системы, интерфейсы взаимодействия компонентов системы, группы пользователей, а также другие поясняющие материалы приведены в Приложении А.

# Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

Таблица 7 - Негативные последствия от реализации угроз безопасности информации

|  |  |  |
| --- | --- | --- |
| **№** | **Виды**  **риска (ущерба)** | **Возможные типовые негативные**  **последствия** |
| У1 | Ущерб физическому лицу | 1. Нарушение конфиденциальности (утечка) персональных данных. 2. Разглашение персональных данных граждан |
| У2 | Риски юридическому лицу, связанные с хозяйственной деятельностью | 1. Неполучение ожидаемой (прогнозируемой) прибыли. 2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. 3. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). 4. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. 5. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. 6. Потеря клиентов, поставщиков. 7. Потеря конкурентного преимущества. 8. Причинение имущественного ущерба. 9. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). 10. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) |

# Возможные объекты воздействия угроз безопасности информации

# Таблица 8 – Объекты воздействия угроз

|  |  |  |
| --- | --- | --- |
| **Негативные последствия** | **Объекты воздействия** | **Виды воздействия** |
| Разглашение  персональных данных  граждан | Главный компьютер | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Нарушение  конфиденциальности  (утечка) персональных  данных. | 1С«Аптека» | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Неполучение  ожидаемой  (прогнозируемой)  прибыли. | Главный компьютер  1С«Аптека» | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Необходимость  дополнительных  (незапланированных)  затрат на закупку  товаров, работ или  услуг (в том числе  закупка программного  обеспечения,  технических средств,  вышедших из строя,  замена, настройка,  ремонт указанных  средств) (У2) | Главный компьютер  Антивирус Касперского | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Необходимость дополнительных (незапланированных) затрат на восстановление деятельности (У2) | Главный компьютер  Антивирус Касперского  1С«Аптека» | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Потеря клиентов, поставщиков (У2) | Главный компьютер  Антивирус Касперского  1С«Аптека» | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Нарушение деловой репутации (У2) | Главный компьютер  Антивирус Касперского  1С«Аптека» | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части. |
| Причинение имущественного ущерба (У2) | Главный компьютер | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) (У2) | 1С«Аптека» | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) (У2) | Главный компьютер  1С«Аптека»» | Блокировка, изменение и/или хищение информации. Шантаж, разглашение информации |

К модели угроз безопасности информации может прилагаться схема с отображением объектов воздействия и их назначения в составе архитектуры системы и сетей.

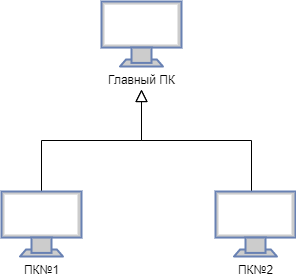


Рисунок 1 Объекты воздействия и их назначения

# Источники угроз безопасности информации

Таблица 9 Источники угроз безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **вида** | **Виды**  **нарушителя** | **Категории**  **нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| 1 | Поставщики вычислительных услуг, услуг связи | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия. |
| 2 | Разработчики программных, программно-аппаратных средств | Внутренний | Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки.  Получение конкурентных преимуществ.  Получение финансовой или иной материальной выгоды.  Непреднамеренные, неосторожные или неквалифицированные действия |
| 3 | Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | Внешний | Получение финансовой или иной материальной выгоды.  Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ |
| 4 | Лица, привлекаемые для установки, настройки. | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ |
| 5 | Отдельные физические лица (хакеры) | Внутренний | Передача конфиденциальной информации третьим лицам; Передача информации о юридическом лице третьим лицам; Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); |
| 6 | Авторизованный пользователь системы | Внутренний | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации (подтверждение статуса).  Месть за ранее совершенные действия.  Непреднамеренные, неосторожные или неквалифицированные действия |
| 7 | Бывшие работники (пользователи) | Внешний | Получение финансовой или иной материальной выгоды.  Месть за ранее совершенные действия |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Виды**  **нарушителей** | **Возможные цели реализации угроз безопасности информации** | | | **Соответствие целей видам риска (ущерба) и возможным негативным последствиям** |
| **Нанесение ущерба физическому лицу** | **Нанесение ущерба юридическому лицу** | **Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности** |
| Поставщики  вычислительных  услуг, услуг связи | - | + | **-** | **У2**Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. |
| Отдельные физические лица (хакеры) | + | **+** | **-** | У1 (Нарушение личной, семейной тайны, утрата чести и доброго имени.)  У2(Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса) |
| Разработчики программных, программно-аппаратных средств | **-** | **+**  (получение финансовой выгоды за счет кражи и коммерческой тайны) | **-** | У2  (утечка коммерческой тайны;  потеря клиентов) |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систему | - | **+** | - | У2(Простой информационной системы или сети) |
| Лица, привлекаемые для установки, настройки. | **-** | **+** | **-** | У2 (Простой информационной системы или сети) |
| Авторизованный пользователь системы | **+** | **+** | **-** | У1 (Нарушение конфиденциальности (утечка) персональных данных)  У2 (Срыв запланированной сделки с партнером) |
| Бывшие работники (пользователи) | - | + | **-** | У2  (утечка коммерческой тайны) |

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Уровень возможностей**  **нарушителей** | **Возможности нарушителей по реализации угроз безопасности информации** | **Виды нарушителей** |
| Н1 | Нарушитель, обладающий базовыми возможностями | Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты.  Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов.  Обладает базовыми компьютерными знаниями и навыками на уровне пользователя.  Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. | Физическое лицо (хакер)  Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем  Лица, обеспечивающих систем (администрация, охрана, уборщики и т.д.)  Авторизованные пользователи систем и сетей  Бывшие работники (пользователи) |
| Н2 | Нарушитель, обладающий базовыми повышенными возможностями | Обладает всеми возможностями нарушителей с базовыми возможностями.  Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз.  Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей.  Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации.  Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. | Преступные группы (два лица и более, действующие по единому плану)  Конкурирующие организации  Лица, привлекаемые для установки, настройки. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Виды риска (ущерба) и возможные негативные последствия\*** | **Виды**  **актуального нарушителя\*\*** | **Категория**  **нарушителя** | **Уровень возможностей**  **нарушителя** |
| 1 | У1:  нарушение конфиденциальности персональных данных граждан;  нарушение личной, семейной тайны, утрата чести и доброго имени;  финансовый, иной материальный ущерб физических лиц | Отдельные физические лица (хакеры) | Внешний | Н2 |
| Системные администраторы и администраторы безопасности | Внутренний | Н2 |
| Авторизованные пользователи систем и сетей | Внутренний | Н2 |
| Конкурирующие организации | Внешний | Н2 |
| 2 | У2:  невозможность заключения договоров, соглашений;  утечка коммерческой тайны;  потеря клиентов;  нарушение деловой репутации;  неполучение ожидаемой прибыли | Лица, привлекаемые для установки, настройки | Внутренний | Н2 |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систему | Внутренний | Н2 |
| Преступные группы  (криминальные структуры) | Внешний | Н2 |
| Разработчики программных, программно-аппаратных средств | Внутренний | H2 |
| Отдельные физические лица (хакеры) | Внешний | Н2 |
| Системные администраторы и администраторы безопасности | Внутренний | Н2 |

# Способы реализации (возникновения) угроз безопасности информации

Таблица 10 - Способы реализации угроз безопасности информации

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Вид нарушителя** | **Категория нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| 1 | Отдельные физические лица (хакеры) (Н2) | Внешний | Удаленное автоматизированное рабочее место (АРМ) пользователя:  несанкционированный доступ к операционной системе АРМ пользователя;  нарушение конфиденциальности информации, содержащейся на АРМ пользователя | Доступ через АРМ | Внедрение вредоносного программного обеспечения |
| Съемные машинные носители информации, подключаемые к АРМ пользователя | Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя |
| 2 | Авторизованный пользователь системы (Н1) | Внутренний | АРМ касса:  модификация платежных поручений, хранящихся на АРМ касса | Локальная вычислительная сеть организации | Ошибочные действия в ходе настройки АРМ главного бухгалтера |
| 3 | Преступные группы (криминальные структуры) (Н2) | Внешний | Размещение программно-аппаратных закладок в помещениях | Удаленное управление | Разглашение конфиденциальной информации |
| 4 | Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (Н2) | Внешний | Поставка оборудования с закладками | Удаленное управление | Считывание данных с АРМ |
| 5 | Лица, привлекаемые для установки, настройки. (Н2) | Внутренний | АРМ касса: заданы неверные параметры работы системы | Интерфейс программы 1С | Внедрение вредоносного программного обеспечения |
| 8 | Конкурирующие организации (Н2) | Внешний | Перехват информации по техническому каналу | Технические средства | Утечка информации |
| 9 | Бывшие работники (пользователи) | Внешний | Получение финансовой или иной материальной выгоды.  Месть за ранее совершенные действия | Доступ через АРМ | Внедрение вредоносного программного обеспечения |
| Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя |

# Актуальные угрозы безопасности информации

Таблица 11 – Актуальные угрозы безопасности информации

|  |  |  |
| --- | --- | --- |
| **№** | **Тактика** | **Основные техники** |
| 1 | Сбор информации о системах и сетях  Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации | 1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций |
| 1.2. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора. |
| 1.3. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей. |
| 2 | Получение первоначального доступа к компонентам систем и сетей  Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий | 2.1. Эксплуатация уязвимостей компонентов систем и сетей при локальной атаке. |
| 2.2. Несанкционированное подключение внешних устройств. |
| 2.2. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими) |
| 3 | Внедрение и исполнение вредоносного программного обеспечения в системах и сетях  Тактическая задача: получив доступ к узлу сети или системы, нарушитель стремится внедрить в его программную среду инструментальные средства, необходимые ему для дальнейших действий | 3.1. Подмена файлов легитимных программ и библиотек непосредственно в системе. |
| 3.2. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п. |
| 4 | Закрепление (сохранение доступа) в системе или сети  Тактическая задача: получив доступ к узлу сети с помощью некоторой последовательности действий, нарушитель стремится упростить себе повторное получение доступа к этому узлу, если он ему впоследствии понадобится (например, устанавливает средства удаленного управления узлом, изменяет настройки средств защиты и другие действия) | 4.1. Несанкционированное создание учетных записей или кража существующих учетных данных |
| 4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети |
| 5 | Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ  Тактическая задача: внедрив вредоносное программное обеспечение или обеспечив постоянное присутствие на узле сети, нарушитель стремится автоматизировать управление внедренными инструментальными средствами, организовав взаимодействия скомпрометированным узлом и сервером управления, который может быть размещен в сети Интернет или в инфраструктуре организации | - |
|
|
|
|
|
|
|
|
|
|
|
|
| 6 | Повышение привилегий по доступу к компонентам систем и сетей  Тактическая задача: получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, нарушитель стремится повысить полученные привилегии и получить контроль над узлом | 6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти. Данные для авторизации включают пароли, хэш-суммы паролей |
| 6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи |
| 6.3 Эксплуатация уязвимостей ПО к повышению привилегий. |
| 7 | Сокрытие действий и применяемых при этом средств от обнаружения  Тактическая задача: нарушитель стремится затруднить применение мер защиты информации, которые способны помешать его действиям или обнаружить их | 7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения. |
| 7.2. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей |
| 7.3. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков |
| 8 | Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям  Тактическая задача: получив доступ к некоторым узлам инфраструктуры, нарушитель стремится получить доступ к другим узлам. Подобное распространение доступа может быть нецеленаправленным: так, еще не зная, к каким именно компонентам инфраструктуры требуется получить доступ для того, чтобы вызвать нужные ему негативные последствия, нарушитель может стремиться получить контроль над как можно большей частью инфраструктуры систем и сетей | - |
| Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз  Тактическая задача: в ходе реализации угроз безопасности информации, нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия | 9.1. Вывод информации через съемные носители |
| 10 | Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям  Тактическая задача: достижение нарушителем конечной цели, приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий | 10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках |

Схемы с отображением сценариев реализации угроз безопасности информации приведены в приложении.

Приложения

Приложение А. Схемы и рисунки, иллюстрирующие состав и архитектуру систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы.

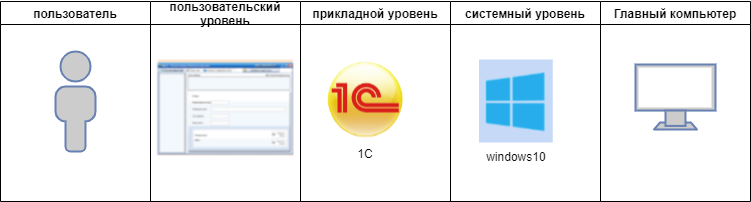


Рисунок 2 Приложение А

Приложение Б. Схемы с отображением типов логических, физических интерфейсов объектов воздействия, в том числе требующих физического доступа к ним, а также соответствующие им способы реализации угроз безопасности информации приведены в приложении

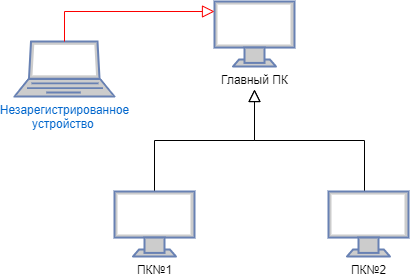


Рисунок 3 Приложение Б