УТВЕРЖДАЮ

Генеральный директор

АО «Ромашка»

ФИО

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

Модель угроз и нарушителя

безопасности информации объекта КИИ

«Pharmacy»

АО «Ромашка»

(ПРОЕКТ)

Разработали студенты группы П-32:

Селезнева Валерия

Утева Александра

2021

1. **Общие положения**

Настоящий документ содержит актуальные угрозы безопасности информации «Pharmacy» АО «Ромашка» (далее – «Pharmacy») значимого объекта критической информационной инфраструктуры \_ категории (далее – ЗОКИИ), которые должны быть заблокированы (нейтрализованы) путем принятия организационно-технических и режимных мер по защите информации. Настоящий документ разработан с учётом положений модели угроз н нарушителя безопасности информации АО «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 ЗОКИИ.

В документе учтены результаты проведённого обследования ЗОКИИ, а также особенности структурно-функциональных характеристик ЗОКИИ АО «Ромашка».

* 1. **Назначение и область действия документа**

Настоящий документ предназначен для определения и оценки угроз безопасности информации ЗОКИИ. 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.

* 1. **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 н 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 канатам 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 АО «Ромашка»:

* Политика информационной безопасности АО «Ромашка», утвержденная приказом от 28.10.2013;
* Политика АО «Ромашка» в области обработки и обеспечения безопасности персональных данных, утверждена приказом № 2020Д от 20.03.2019
* Концепция построения системы информационной безопасности, утвержденная приказом от 29.11.2013;
* А.01.00.2019, утверждено приказом № 582ОД(а) от 26.07.2019
* 10.01- 90-2014 Положение об информационно-новостных ресурсах АО «Ромашка», утверждено приказом № \_\_ от 06.11.2014
* 10.01-2018 Положение о порядке организации совещаний в АО «Ромашка», утверждено приказом № \_\_ от 26.06.2018
* 11-015 Положение о порядке проведения переговоров с потенциальными заказчиками, утверждено приказом № \_\_ от 10.06.2015
* 20- 2014 Положение о порядке применения паролей доступа для обеспечения информационной безопасности АО «Ромашка», утверждено приказом № \_ от 21.04.2014
* 0- -2014 Положение о прядке безопасности использования внешней электронной почты в АО «Ромашка», утверждено приказом № \_\_ от 21.04.2014
* 0- 2014 «Положение о порядке безопасного использования ресурсов сети Интернет в АО «Наименование», утверждено приказом № \_\_\_ от 21.04.2014
* 0- -2014 «Положение о порядке антивирусной защиты в АО «Ромашка», утверждено приказом № \_ от 01.11.2013
* 14 Положение «Порядок обеспечения эксплуатации и обслуживания средств вычислительной техники и программного обеспечения», утверждено приказом № \_ от 15.10.2014
* .1144-2016 Положение процедура управления информационными активами в АО «Ромашка», утверждено приказом № \_\_ от 06.06.2016
* .1145-2016 Внедрение и эксплуатация информационных систем в АО «Ромашка», утверждено приказом № \_\_ от 06.06.2016
* 27.1014-2016 «Положение о коммерческой тайне АО «Ромашка», утверждено приказом № \_\_ от 29.06.2016
* -2014 Положение об управлении доступом к ресурсам корпоративной сети АО «Ромашка», утверждено приказом № \_ от 27.08.2014
* -2015 Положение об аудите информационной безопасности, утверждено приказом № \_\_ от 25.03.2015
* 2015 Положение о безопасном использовании съемных носителей информации в АО «Ромашка», утверждено приказом № \_\_ от 26.06.2015
* 1143-2016 Положение. Безопасное использование мобильных средств вычислительной техники, утверждено приказом № \_\_ от 16.06.2016
* -2017 Безопасность сетевой инфраструктуры в АО «Ромашка», утверждено приказом № \_\_ от 15.02.2017
* 1194-2017 Управление рисками информационной безопасности АО «Ромашка», утверждено приказом № \_\_ от 24.11.2017
* .1238-2018 Положение. Административно – управленческие вопросы, система управления. Обучение работников в целях повышения осведомленности в области информационной безопасности в АО «Ромашка», утверждено приказом № \_\_ от 03.07.2018
* .00.1239 Положение. Административно – управленческие вопросы, система управления. Управление инцидентами информационной безопасности. Порядок реагирования и устранения, утверждено приказом № 669 от 09.07.2018
* .3084 Административно – управленческие вопросы. Правила, особенности и порядок работы с конфиденциальной информацией, утверждены приказом № 669 от 09.07.2018
* .3274-2019 Положение. Информационные технологии. Управление изменениями информационных систем
* Положение о порядке работы с соглашениями о конфиденциальности, утверждено приказом № \_\_ ОД от 05.06.2019
* -2016 Регламент «Порядок установки обновлений СУБД и ППО в АО «Наименование», утвержден приказом № \_\_ от 30.03.2016
* -2016 Регламент «Процедура управления изменениями в сетевой инфраструктуре», утвержден приказом № \_\_ от 11.04.2016
* Регламент управления уязвимостями информационных систем в АО «Наименование», утвержден приказом № \_\_\_ от 18.12.2015
* Регламент резервного копирования, утвержден приказом № \_\_ от 27.11.2013
* .4048-2018 Инструкция работника по правилам безопасного хранения электронных документов в АО «Ромашка», утверждена приказом № \_\_\_ от 24.12.2018
* Инструкция по обеспечению безопасности эксплуатации СКЗИ, утверждена приказом № \_\_ от 16.01.2018
* Инструкция о пропускном и внутриобъектовом режимах в АО «Наименование», утверждена приказом № \_\_ от 28.04.2015
* Перечень сведений конфиденциального характера АО «Ромашка», утвержден приказом № \_\_ ОД от 03.04.2019
* Цели в области информационной безопасности АО «Ромашка», утверждены приказом № \_\_ ОД от 04.04.2019
* Приказ № \_\_ от 22.04.2014 «О хранении электронных и производственных данных»;
* Приказ № \_\_ от 10.04.2015 «Об организации обмена конфиденциальной документации с филиалами»;
* Приказ № \_\_\_ от 07.09.2016 «О передаче служебной информации по открытым каналам связи»
* Приказ № \_\_\_ от 25.06.2014 «Об использовании электронной почты, сети интернет и электронных носителей»
* Приказ № \_\_\_ от 28.12.2018 «О пересылке конфиденциальной информации»
* Приказ № \_\_ от 13.12.2018 «О внедрении стандарта по обеспечению информационной безопасности»
* Приказ № \_\_ от 12.12.2019 «О защите информации»
  1. **Наименование обладателя информации, заказчика, оператора систем и сетей**

Заказчиком и обладателем информации является АО «Ромашка».

* 1. **Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей**

Инженер по обеспечению безопасности.

* 1. **Наименование организации, привлекаемой для разработки модели угроз безопасности информации**

Модель угроз безопасности информации АО «Ромашка» разработана с привлечением АО «11111», имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциально информации (рег. № \_\_\_ от \_\_\_\_).

1. **Описание систем и сетей и их характеристика как объектов защиты**
   1. **Описание системы «Pharmacy»**

«Pharmacy» создана и функционирует в соответствие с приказом № \_\_ от \_\_.\_\_.\_\_ «О вводе в эксплуатацию», утвержденного генеральным директором АО «Ромашка».

«Pharmacy» размещается в пределах контролируемой зоны АО «Ромашка» по адресу г. Зеленоград, дом 1 и предназначена для учета препаратовбиб и посетителей. В ней обрабатывается общедоступная информация и информация конфиденциального характера, в соответствие с Перечнем сведений конфиденциального характера АО «Ромашка», утвержден приказом № \_\_\_ от 03.04.2019, информация, циркулирующая в «Pharmacy», отнесена к общедоступной, технологической информации, коммерческой тайне, служебной информации, информации с пометкой «Для служебного пользования».

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

* Учет препаратов в аптеке;
* Учет выданных препаратов посетителям;
* Учет посетителей;

В соответствие с:

Актом классификации № \_\_ от \_\_.\_\_.\_\_« Pharmacy» присвоен класс защищенности 2;

Актом категорирования объектов критической информационной инфраструктуры № \_\_ от \_\_.\_\_.\_\_ «Pharmacy» отнесена к 0 категории ЗОКИИ.

Актом определения уровня защищенности ПДн № \_\_ от \_\_.\_\_.\_\_ «Pharmacy» присвоен уровень защищенности 2.

* 1. **Состав «Pharmacy»**

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

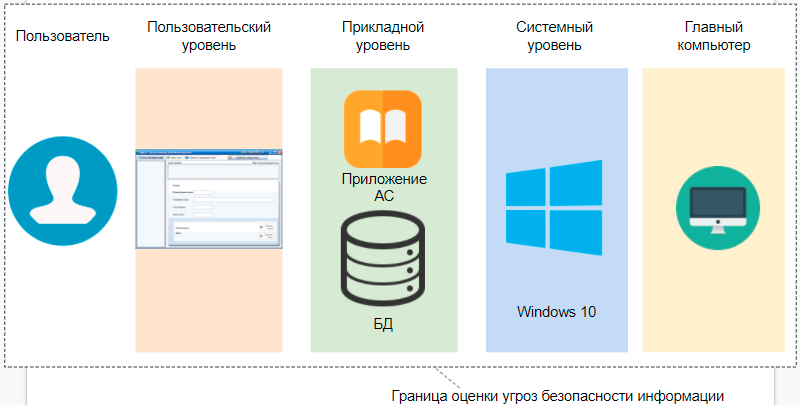
Таблица 1 – Состав ТС «Pharmacy»

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

Таблица 2 –Перечень ПО «Pharmacy»

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Примечание** |
| 1 | Приложение АС |  |
| 2 | Операционная система Windows 10 |  |
| 3 | База данных |  |
| 4 | Антивирус Касперского |  |

* 1. **Описание архитектуры «Pharmacy»**



* 1. **Описание пользователей «Pharmacy»**
     1. **Внешние пользователи**

Отсутствуют

* + 1. **Внутренние пользователи**

Все внутренние пользователи наделены равными полномочиями:

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

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

Разграничение прав доступа назначается в соответствии с Разрешительной системы доступа к ОКИИ.

* 1. **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 АО «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 систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы приведены в Приложении А.

1. **Возможные негативные последствия от цели реаии (возникновения) угроз безопасности информации**

|  |  |  |
| --- | --- | --- |
| **№** | **Виды**  **риска (ущерба)** | **Возможные типовые негативные**  **последствия** |
| **У1** | Ущерб физическому лицу | Разглашение персональных данных граждан  Нарушение конфиденциальности (утечка) персональных данных. |
| У2 | Риски юридическому лицу, связанные с хозяйственной деятельностью | Недополучение ожидаемой (прогнозируемой) прибыли.  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.  Потеря клиентов, поставщиков.  Нарушение деловой репутации.  Причинение имущественного ущерба.  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).  Утечка конфиденциальной информации (коммерческой тайны, секретов производства  (ноу-хау) и др.) |

1. **Возможные объекты воздействия угроз безопасности информации**

Таблица

|  |  |  |
| --- | --- | --- |
| **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. | База данных |
| Приложение АС |
| Недополучение ожидаемой (прогнозируемой) прибыли. | Главный компьютер | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| База данных |
| Приложение АС |
| 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 | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| Антивирус Касперского |
| Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса (У2) | Главный компьютер | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| База данных |
| Приложение АС |
| Необходимость дополнительных (незапланированных) затрат на восстановление деятельности (У2) | Главный компьютер | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| База данных |
| Приложение АС |
| Антивирус Касперского |
| Потеря клиентов, поставщиков (У2) | Главный компьютер | Блокировка, изменение и/или хищение информации. Шантаж, разглашение информации |
| База данных |
| Приложение АС |
| Антивирус Касперского |
| Нарушение деловой репутации (У2) | Главный компьютер | Блокировка, изменение и/или хищение информации. Шантаж, разглашение информации |
| База данных |
| Управляющее приложение |
| Антивирус Касперского |
| 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) | Приложение АС | Деструктивное воздействие на сетевое оборудование и/или программное обеспечение, с наихудшим результатом в виде неработоспособности всей системы или ее части |
| База данных |
| Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) (У2) | Главный компьютер | Блокировка, изменение и/или хищение информации. Шантаж, разглашение информации |
| База данных |
| Приложение АС |

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



1. **Источники угроз безопасности информации**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **вида** | **Виды**  **нарушителя** | **Категории**  **нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| 1 | Поставщики вычислительных услуг, услуг связи | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия. |
| 2 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием;  Непреднамеренные, неосторожные или неквалифицированные действия |
| 3 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | 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);  Непреднамеренные, неосторожные или неквалифицированные действия;  Месть за ранее совершенные действия |
| 4 | Авторизованные пользователи систем и сетей | 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);  Непреднамеренные, неосторожные или неквалифицированные действия;  Месть за ранее совершенные действия |
| 5 | Разработчики программных, программно-аппаратных средств | Внутренний | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки |
| 6 | 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); |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | **-** | **+**  **(**Непреднамеренные, неосторожные или неквалифицированные действия.) | **-** | **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. |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | **-** | **+**  (Причинение имущественного ущерба путем обмана или злоупотребления доверием;  Непреднамеренные, неосторожные или неквалифицированные действия) | **-** | **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. |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | +  (Передача конфиденциальной информации третьим лицам;  Месть за ранее совершенные действия) | **+**  (Передача информации о юридическом лице третьим лицам,  любопытство или желание самореализации;  Месть за ранее совершенные действия;  Причинение имущественного ущерба путем обмана или злоупотребления доверием;  Непреднамеренные, неосторожные или неквалифицированные действия) | **-** | **У1**  Нарушение конфиденциальности (утечка) персональных данных.  Разглашение персональных данных граждан  **У2**  Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)  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.  Потеря клиентов, поставщиков.  Нарушение деловой репутации.  Причинение имущественного ущерба.  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). |
| Авторизованные пользователи систем и сетей | +  (Передача конфиденциальной информации третьим лицам;  Месть за ранее совершенные действия) | **+**  (Передача информации о юридическом лице третьим лицам,  любопытство или желание самореализации;  Месть за ранее совершенные действия;  Непреднамеренные, неосторожные или неквалифицированные действия) | **-** | **У1**  Нарушение конфиденциальности (утечка) персональных данных.  Разглашение персональных данных граждан  **У2**  Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)  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.  Потеря клиентов, поставщиков.  Нарушение деловой репутации.  Причинение имущественного ущерба.  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). |
| Разработчики программных, программно-аппаратных средств | - | **-** | **-** | - |
| Отдельные физические лица (хакеры) | +  (Передача конфиденциальной информации третьим лицам;  Получение финансовой или иной материальной выгоды;  Любопытство или желание самореализации (подтверждение статуса)) | **+**  **(**Передача информации о юридическом лице третьим лицам;  Получение финансовой или иной материальной выгоды;  Любопытство или желание самореализации (подтверждение статуса)) | **-** | **У1**  Разглашение персональных данных граждан  Нарушение конфиденциальности (утечка) персональных данных.  **У2**  Недополучение ожидаемой (прогнозируемой) прибыли.  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.  Потеря клиентов, поставщиков.  Нарушение деловой репутации.  Причинение имущественного ущерба.  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).  Утечка конфиденциальной информации (коммерческой тайны, секретов производства  (ноу-хау) и др.) |
|

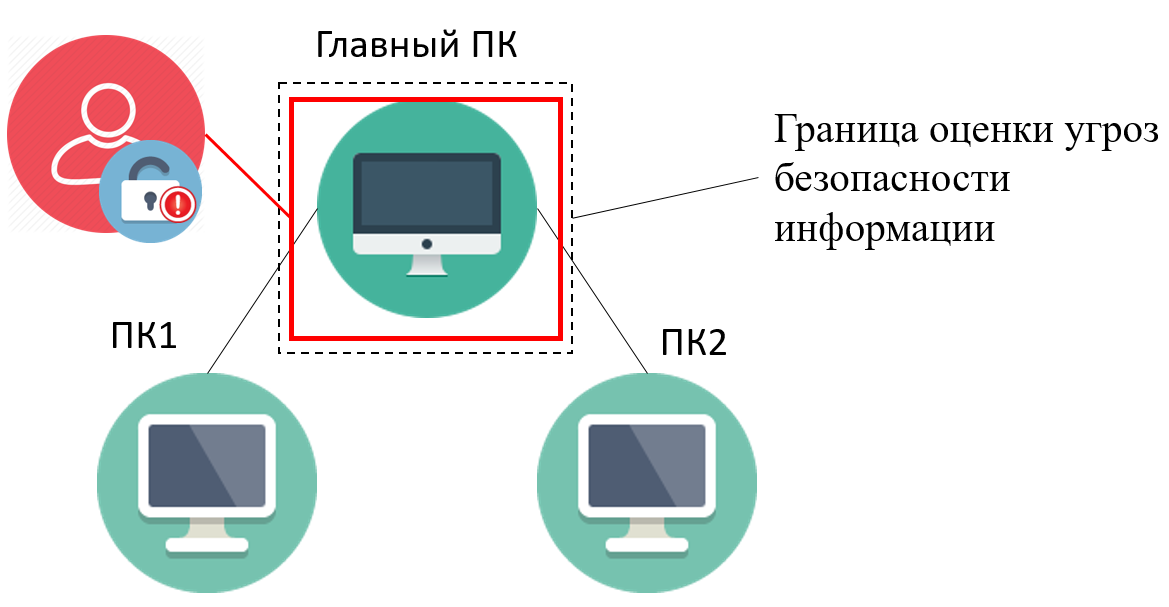
|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Уровень возможностей**  **нарушителей** | **Возможности нарушителей по реализации угроз безопасности информации** | **Виды нарушителей** |
| Н1 | Нарушитель, обладающий базовыми возможностями | Имеет возможность при реализации угроз безопасности информации 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.  **Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов** | Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.)  Авторизованные пользователи систем и сетей |
| 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.  **Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей** | Поставщики вычислительных услуг, услуг связи  Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ  Отдельные физические лица (хакеры) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Виды риска (ущерба) и возможные негативные последствия\*** | **Виды**  **актуального нарушителя\*\*** | **Категория**  **нарушителя** | **Уровень возможностей**  **нарушителя** |
| 1 | У1:  Нарушение конфиденциальности (утечка) персональных данных.  Разглашение персональных данных граждан | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Н1 |
| Авторизованные пользователи систем и сетей | Внутренний | Н1 |
| Отдельные физические лица (хакеры) | Внутренний | Н2 |
| 2 | У2:  Недополучение ожидаемой (прогнозируемой) прибыли.  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.  Потеря клиентов, поставщиков.  Нарушение деловой репутации.  Причинение имущественного ущерба.  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).  Утечка конфиденциальной информации (коммерческой тайны, секретов производства  (ноу-хау) и др.) | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Н1 |
| Авторизованные пользователи систем и сетей | Внутренний | Н1 |
| Поставщики вычислительных услуг, услуг связи | Внутренний | Н2 |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Н2 |
| Отдельные физические лица (хакеры) | Внутренний | Н2 |

1. **Способы реализации (возникновения) угроз безопасности информации**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Вид нарушителя** | **Категория нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| 1 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Приложение АС:  несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;  утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных | Пользовательский интерфейс приложения АС | Доступ к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хэша пароля, для восстановления сеанса |
| Пользовательский интерфейс приложения АС | Прохождение нарушителем процедуры авторизации на основе полученной из открытых источников  или от информационного сервиса идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. |
| Пользовательский интерфейс приложения АС | Получение нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). |
| Пользовательский интерфейс приложения АС | Неправомерное получение нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). |
| Главный компьютер:  нарушение функционирования (работоспособности) средств обработки и хранения информации; | Пользовательский интерфейс ОС Windows 10 | Сброс пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом |
| 2 | Авторизованные пользователи систем и сетей | Внутренний | Приложение АС:  утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных;  повреждение защищаемой информации | Пользовательский интерфейс приложения АС | Удаление из хранилища некоторых обрабатываемых данных без уведомления конечного пользователя или администратора |
| Пользовательский интерфейс приложения АС | Неправомерное получение нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). |
| Внешний носитель:  утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных;  повреждение защищаемой информации | Неконтролируемый доступ к информации на внешнем носителе | Раскрытие информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). |
| Стандартные средства ОС для работы с внешними носителями | Утрата хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации. |
| ОС Windows 10:  повреждение защищаемой информации | Стандартные системные и сетевые утилиты | Деструктивное программное воздействие на систему за счёт использования имеющихся или предварительно внедрённых стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети) |
| 3 | Поставщики вычислительных услуг, услуг связи | Внутренний | Главный компьютер:  нарушение функционирования (работоспособности) средств обработки и хранения информации; | Пользовательский интерфейс ОС Windows 10 | Сброс пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного осуществления перезагрузки отдельных устройств, блоков или системы в целом |
|
| 4 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Главный компьютер:  нарушение функционирования (работоспособности) средств обработки и хранения информации; | Пользовательский интерфейс ОС Windows 10 | Сброс пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом |
|
| Приложение АС:  несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;  утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных | Пользовательский интерфейс приложения АС | Доступ к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хэша пароля, для восстановления сеанса |
| Пользовательский интерфейс приложения АС | Прохождение нарушителем процедуры авторизации на основе полученной из открытых источников  или от информационного сервиса идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. |
| Пользовательский интерфейс приложения АС | Получение нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). |
| Пользовательский интерфейс приложения АС | Неправомерное получение нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). |
| 5 | Отдельные физические лица (хакеры) | Внутренний | Главный компьютер:  несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;  нарушение функционирования (работоспособности) средств обработки и хранения информации; модификация (подмена) защищаемой информации, системных, конфигурационных, иных служебных данных | Материнская плата Главного компьютера | Сброс паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера») |
| Пользовательский интерфейс BIOS | Неправомерное использование декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера |
| Пользовательский интерфейс BIOS | Подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы |
| Пользовательский интерфейс BIOS | Осуществление нарушителем несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера путём ввода «пустого» пароля |
| Вредоносные программы, установленные с внешнего носителя | Дезинформирование пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства |
| Вредоносные программы, установленные с внешнего носителя | Прямой доступ (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации |
| Приложение АС:  несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;  утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных | Пользовательский интерфейс приложения АС | Доступ к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хэша пароля, для восстановления сеанса |
| Пользовательский интерфейс приложения АС | Прохождение нарушителем процедуры авторизации на основе полученной из открытых источников  или от информационного сервиса идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. |
| Пользовательский интерфейс приложения АС | Получение нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). |
| Пользовательский интерфейс приложения АС | Неправомерное получение нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). |
| Пользовательский интерфейс доступа к данным пользователя | Угроза заключается в возможности доступа к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хэша пароля, для восстановления сеанса |
| ОС Windows 10:  несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;  нарушение функционирования (работоспособности) средств обработки и хранения информации; модификация (подмена) защищаемой информации, системных, конфигурационных, иных служебных данных | Пользовательский интерфейс файловой системы Windows 10 | Получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения).  Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы |
| Пользовательский интерфейс ОС Windows | Деструктивное программного воздействие на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами. |
| База данных:  несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным;  нарушение функционирования (работоспособности) средств обработки и хранения информации; модификация (подмена) защищаемой информации, системных, конфигурационных, иных служебных данных | Вредоносные программы, установленные с внешнего носителя | Внесение нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы Microsoft Windows, а любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью |
| Вредоносные программы, установленные с внешнего носителя | Нарушение доступности части функционала или всей информационной системы из-за повреждения используемого в её работе реестра вследствие некорректного завершения работы операционной системы (неконтролируемая перезагрузка, возникновения ошибок в работе драйверов устройств и т.п.), нарушения целостности файлов, содержащих в себе данные реестра, возникновения ошибок файловой системы носителя информации или вследствие осуществления нарушителем деструктивного программного воздействия на файловые объекты, содержащие реестр |
|  | Вредоносные программы, установленные с внешнего носителя | Нарушение целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём |

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.



1. **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 |
| 10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа |
| 10.3. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей |