УТВЕРЖДАЮ

Руководитель органа государственной власти (организации) или иное уполномоченное лицо \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

Модель угроз безопасности ИСПДн АНО ДПО ЦО "ПрофСтандарт"

# Основные положения

Настоящий документ разработан в соответствии с требованием п. 7 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

Определение нарушителей и угроз безопасности персональных данных при их обработке и последующее формирование на их основе модели угроз и нарушителей является одним из необходимых мероприятий по обеспечению безопасности ПДн в информационных системах.

Выявление и учет угроз безопасности ПДн в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в информационных системах ПДн.

Настоящая Модель угроз и нарушителей учитывает требования следующих законодательных актов и нормативно-методических документов:

− Федеральный закон №152-ФЗ от 27 июля 2006 года «О персональных данных»;

− постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

− Приказ ФСТЭК Российской Федерации № 21 от 18.02.2013 «Состав и содержание технических и организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

− Федеральная служба по техническому и экспортному контролю методический документ методика оценки угроз безопасности информации от 5 февраля 2021 года.

# 2. Описание систем и сетей и их характеристика как объектов защиты

## **Наименование систем и сетей, для которых разработана модель угроз безопасности информации**

Модель угроз разработана для АНО ДПО ЦО "ПрофСтандарт" (далее ПрофСтандарт).

## **Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных**

Класс защищенности ИСПДн - уровень защищенности персональных данных

## **Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети**

ИСПДн создана и функционирует согласно следующим нормативно правовым актам Российской Федерации:

* Федеральному закону «О персональных данных» от 27.07.2006 N 152-ФЗ
* Постановлению Правительства РФ от 15.09.2008 N 687
* Постановлению Правительства Российской Федерации от 1 ноября 2012 г. № 1119
* Приказу ФСТЭК России от 18 февраля 2013 г. № 21.

## **Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим**

ПрофСтандарт является автономной некоммерческой организацией дополнительного профессионального образования.

В ПрофСтандарте обрабатываются и хранятся следующие типы ПДн:

* Фамилия, имя, отчество;
* Год, месяц, дата и место рождения;
* Адрес регистрации и проживания;
* Номер паспорта;
* Должность;
* Номера зарплатных карт;
* ИНН;
* СНИЛС;
* Уровень образования;
* Контактные телефоны;
* Электронная почта;
* Фотография;
* Данные об обучении (курсы, сертификаты, квалификации);
* Трудовая книжка (для сотрудников);
* Воинский учет (для военнообязанных);
* Медицинская книжка (при необходимости);
* Подпись;

## Основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети.

Основными процессами, взаимодействующими с ПДн, в ПрофСтандарте являются: начисление зарплаты, найм на работу, бух отчеты, сбор данных при подаче заявки, заключение договоров на обучение, ведение академических записей, выдача документов об образовании.

## Состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей

ПрофСтандарт состоит из следующих систем и сетей:

* Веб сервер
* Сервер с базой данных
* АРМ сотрудников
* МФУ
* Проекторы

Интерфейсы ИСПДн:

Физические:

1. 22 – SFTP. Протокол защищенной передачи файлов для резервного копирования.
2. 25 – SMTP. Протокол исходящей почтовой рассылки.
3. 53 – DNS. Разрешение доменных имен во внутренней сети.
4. 80 – HTTP. Нешифрованный веб-доступ.
5. 443 – HTTPS. Шифрованный веб-доступ к LMS и порталу.
6. 500/4500 – IPsec/IKE. Туннелирование VPN-соединений.
7. 1433 – MSSQL. Порт связи с MSSQL БД, сервером.

## **Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа.**

Таблица 1 - Матрица доступа

|  |  |  |
| --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные действия |
| Сотрудники отдела кадров | Полный | Ввод, редактирование, хранение, уничтожение кадровых данных |
| Преподавательский состав | Ограниченный | Просмотр данных обучающихся своей группы, внесение оценок и посещаемости |
| Бухгалтерия | Частичный | Обработка финансовых данных (реквизиты карт, ИНН) без права копирования |
| Администраторы IT-систем | Технический | Настройка систем хранения, резервное копирование, восстановление данных (без просмотра содержания) |
| Методический отдел | К обезличенным данным | Анализ статистики успеваемости и эффективности курсов |
| Служба безопасности | Контрольный | Мониторинг действий с ПДн, расследование инцидентов, аудит доступов |
| Обучающиеся | Минимальный | Просмотр и редактирование только своих персональных данных |
| Руководство организации | Полный (контрольный) | Просмотр всех категорий ПДн, утверждение политик доступа и регламентов |

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

Рассматривается атака на похищение персональных данных (Атака проведена успешно).

Таблица 2 – матрица негативных последствий

|  |  |  |
| --- | --- | --- |
| **№** | **Виды риска (ущерба)** | **Негативные последствия** |
| У1 | Ущерб физическому лицу | Нарушение тайны переписки, телефонных  переговоров, иных сообщений.  Финансовый, иной материальный ущерб  физическому лицу.  Нарушение конфиденциальности (утечка)  персональных данных. |
| У2 | Ущерб юридическому лицу | Потеря клиентов, поставщиков.  Потеря конкурентного преимущества.  Невозможность заключения договоров, соглашений.  Нарушение деловой репутации.  Снижение престижа.  Утрата доверия.  Причинение имущественного ущерба.  Неспособность выполнения договорных обязательств.  Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.  Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг.  Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.  Простой информационной системы или сети.  Публикация недостоверной информации на веб-ресурсах организации.  Использование веб-ресурсов для распространения вредоносного ПО.  Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени.  Утечка конфиденциальной информации (коммерческой тайны, ноу-хау и др.).  Нарушение законодательства Российской Федерации.  Потеря (хищение) денежных средств.  Недополучение ожидаемой (прогнозируемой) прибыли.  Срыв запланированной сделки с партнером. |
| У3 | Отсутствуют | Вред государству нанесен быть не может. |

# 4. Возможные объекты воздействия угроз безопасности информации

На рисунке 1 изображена схема сети ПрофСтандарт.

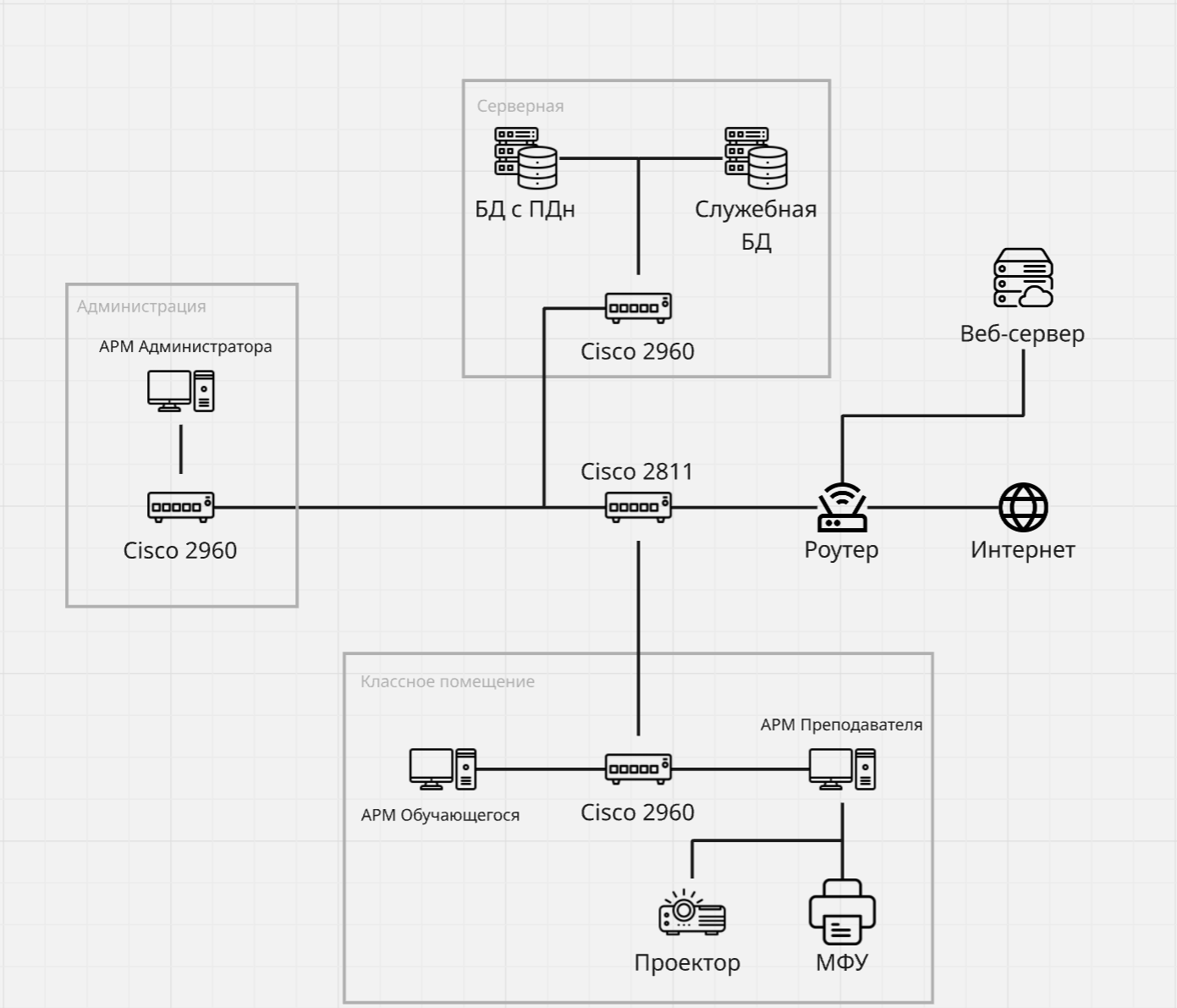


Рисунок 1-схема сети ИСПДн

На рисунке 2 представленном ниже изображена схема потоков информации при помощи DFD (Data Flow Diagram).

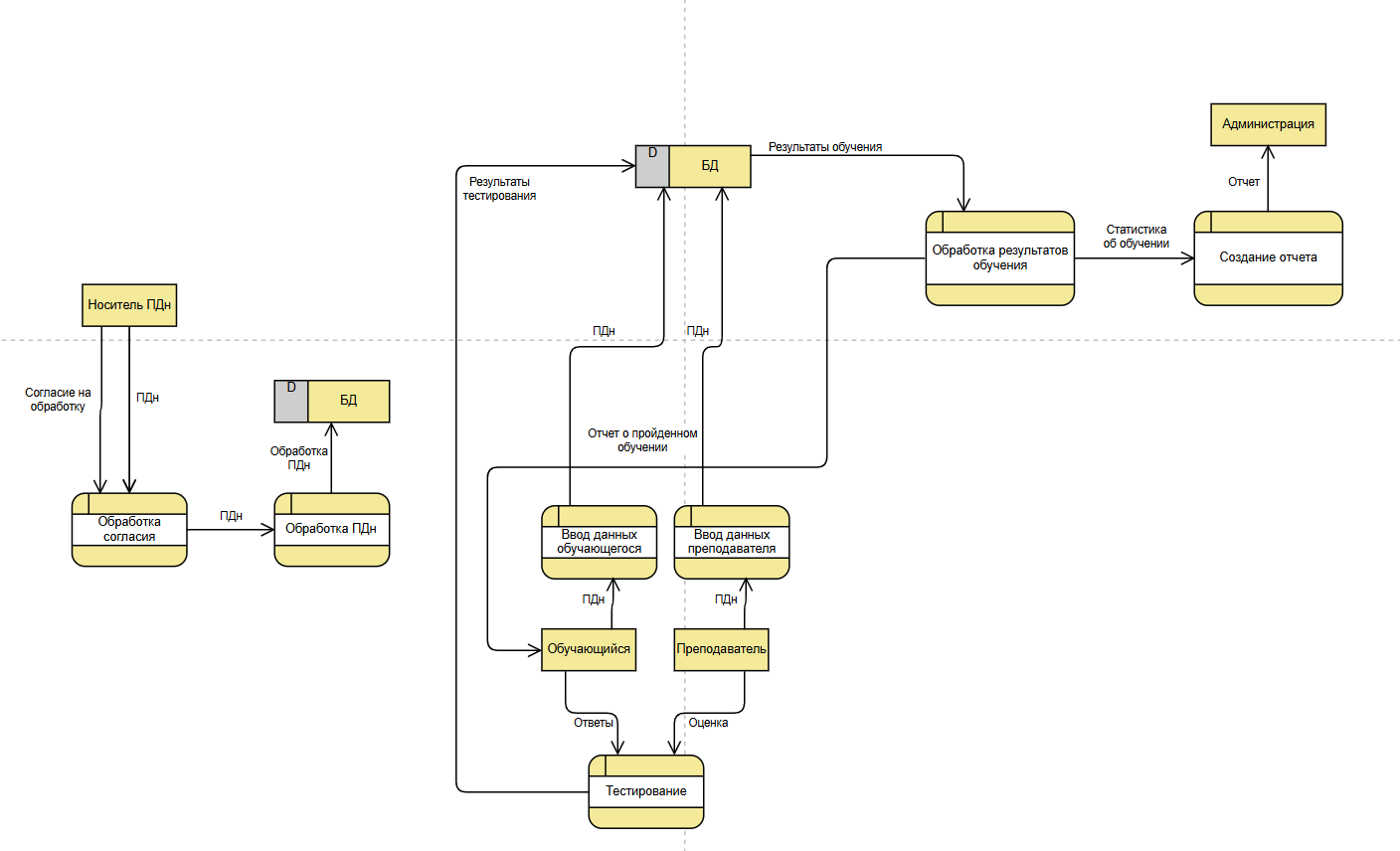


Рисунок 2 - Диаграмма потоков данных

Описание групп информационных ресурсов и компонентов систем и сетей

ПрофСтандарт включает различные компоненты и информационные ресурсы, которые могут подвергаться воздействию угроз:

Группы информационных ресурсов:

Персональные данные обучающихся:

Персональные данные сотрудников: Паспортные данные, налоговые идентификаторы, информация о зарплатах.

Финансовая информация: данные о зарплатных выплатах, банковских реквизитах, платёжных документах.

Компоненты системы и сети: клиентские устройства: Рабочие станции сотрудников, с которых происходит доступ к системе ПрофСтандарта.

Сетевое оборудование: маршрутизаторы, коммутаторы, обеспечивающие связь между компонентами.

Объекты воздействия ПрофСтандарта:

Маршрутизатор cisco 2811: протокол DHCP, SSH.

Коммутаторы cisco 2960: протокол STP, SSH, разделение на vlan.

Сервер: БД с ПДн, Служебная БД. Windows 2012, MSSQL

Веб сервер: Debian.

АРМ Администрации: Windows 10, 1С-Бухгалтерия, Microsoft office.

АРМ Преподавателя: Windows 10, 1С-Бухгалтерия, Microsoft office.

АРМ Обучающегося: Windows 10, Microsoft office.

Таблица 3 – матрица возможных объектов и типов угроз

|  |  |  |
| --- | --- | --- |
| Негативные последствия | Объекты воздействия | Виды воздействия |
| Разглашение ПДн | АРМ Администрации  АРМ Преподавателя АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Финансовый, иной материальный ущерб физическому лицу | АРМ Администрации  АРМ Преподавателя АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);  Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Срыв сделки | АРМ Администрации cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);  Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Отказ в обслуживании компонентов (нарушение доступности);  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;  нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Нарушение законодательства | АРМ Администрации  АРМ Преподавателя АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);  несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Отказ в обслуживании компонентов (нарушение доступности);  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Необходимость доп. затрат | АРМ Администрации  АРМ Преподавателя АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);  несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Отказ в обслуживании компонентов (нарушение доступности);  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Потеря клиентов | АРМ Администрации АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);  несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Отказ в обслуживании компонентов (нарушение доступности);  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Потеря деловой репутации | АРМ Администрации  АРМ Преподавателя АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);  несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Отказ в обслуживании компонентов (нарушение доступности);  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Простой информационной системы или сети | АРМ Администрации  АРМ Преподавателя АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Отказ в обслуживании компонентов (нарушение доступности);  Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |
| Утечка конфиденциальной информации | АРМ Администрации  АРМ Преподавателя АРМ Обучающегося cisco 2811  cisco 2960  БД с ПДн  МФУ | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);  несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;  Отказ в обслуживании компонентов (нарушение доступности);  Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);  Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;  Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации. |

# 5. Источники угроз безопасности информации

Таблица 5 – Источники угроз безопасности информации

|  |  |  |
| --- | --- | --- |
| **Виды**  **нарушителя** | **Категории**  **нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| Преступные группы (криминальные структуры) | Внешний | Получение финансовой или иной материальной выгоды.  Желание самореализации (подтверждение статуса) |
| Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации (подтверждение статуса) |
| Конкурирующие организации | Внешний | Получение конкурентных преимуществ.  Получение финансовой или иной материальной выгоды |
| 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 |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | Внешний | Получение финансовой или иной материальной выгоды.  Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Получение финансовой или иной материальной выгоды.  Непреднамеренные, неосторожные или неквалифицированные действия |
| Авторизованные пользователи систем и сетей | Внутренний | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации (подтверждение статуса).  Месть за ранее совершенные действия.  Непреднамеренные, неосторожные или неквалифицированные действия |
| Системные администраторы и администраторы безопасности | Внутренний | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации (подтверждение статуса).  Месть за ранее совершенные действия.  Непреднамеренные, неосторожные или неквалифицированные действия |
| 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, индивидуальному предпринимателю** | **Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности** |
| Отдельные физические лица (хакеры) | +  Получение прибыли из ПДн людей,  Нарушение конфиденциальности | +  Получение прибыли из служебных данных,  Срыв сделок, временное прекращение деятельности организации | - | У1  Разглашение персональных данных;  Нарушение конфиденциальности;  Финансовый ущерб;  У2  Нарушение деловой репутации;  Финансовый ущерб; |
| Преступные группы (криминальные структуры) | +  Получение прибыли из ПДн людей,  Нарушение конфиденциальности | +  Получение прибыли из служебных данных,  Потеря репутации организации,  Срыв сделок, временное прекращение деятельности организации | - | У1  Разглашение персональных данных;  Нарушение конфиденциальности;  Финансовый ущерб;  У2  Нарушение деловой репутации;  Финансовый ущерб; |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | +  Получение прибыли из ПДн людей,  Нарушение конфиденциальности | +  Получение прибыли из служебных данных,  Потеря репутации организации,  Срыв сделок, временное прекращение деятельности организации | - | У2  Принятие неправильных решений;  Финансовый ущерб; |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | +  Получение прибыли из ПДн людей,  Нарушение конфиденциальности | +  Получение прибыли из служебных данных,  Потеря репутации организации,  Срыв сделок, временное прекращение деятельности организации | - | У2  Принятие неправильных решений;  Финансовый ущерб; |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | +  Получение прибыли из ПДн людей,  Нарушение конфиденциальности | +  Получение прибыли из служебных данных,  Потеря репутации организации,  Срыв сделок, временное прекращение деятельности организации | - | У2  Принятие неправильных решений;  Финансовый ущерб;  Нарушение штатного режима функционирования  автоматизированной системы управления и  управляемого объекта и/или процесса; |
| Авторизованные пользователи систем и сетей | +  Получение прибыли из ПДн людей,  Нарушение конфиденциальности | +  Потеря репутации организации,  Срыв сделок, временное прекращение деятельности организации | - | У1  Разглашение персональных данных;  Нарушение конфиденциальности;  Финансовый ущерб;  У2  Нарушение деловой репутации;  Финансовый ущерб; |
| Системные администраторы и администраторы безопасности | +  Получение прибыли из ПДн людей,  Нарушение конфиденциальности | +  Потеря репутации организации,  Срыв сделок, временное прекращение деятельности организации | - | У1  Разглашение персональных данных;  Нарушение конфиденциальности;  Финансовый ущерб;  У2  Нарушение деловой репутации;  Финансовый ущерб; |

# 6. Способы реализации (возникновения) угроз безопасности информации

таблица 6 - способы реализации угроз

|  |  |  |  |
| --- | --- | --- | --- |
| Вид нарушителя | Объект воздействия | Доступные интерфейсы | Способы реализации |
| Преступные группы (криминальные структуры)  Категория:  Внешний Н2 | Cisco 2811  Cisco 2960 | Интерфейсы удаленного администрирования сетевого оборудования: SSH, Telnet | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; |
| БД с ПДн  Служебная БД | Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); |
| Веб сервер | Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); |
| АРМ работников | Доступ из локальная сеть организации | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; |
| Отдельные физические лица (хакеры)  Категория:  Внешний Н1 | Cisco 2811  Cisco 2960 | Интерфейсы удаленного администрирования сетевого оборудования: SSH, Telnet | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; |
| БД с ПДн  Служебная БД | Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); |
| Веб сервер | Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); |
| АРМ работников | Доступ из локальная сеть организации | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; |
| Конкурирующие организации  Категория:  Внешний Н2 | Cisco 2811  Cisco 2960 | Интерфейсы удаленного администрирования сетевого оборудования: SSH, Telnet | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; |
| БД с ПДн  Служебная БД | Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); |
| Веб сервер | Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); |
| АРМ работников | Доступ из локальная сеть организации | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; |
| Разработчики программных, программно-аппаратных средств  Категория:  Внутренний Н3 | Cisco 2811  Cisco 2960 | Интерфейсы удаленного администрирования сетевого оборудования: SSH, Telnet | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 3. использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств; 4. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; |
| БД с ПДн  Служебная БД | Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; |
| Веб сервер | Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; |
| АРМ работников | Доступ из локальная сеть организации. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем  Категория:  Внешний Н1 | Cisco 2811  Cisco 2960 | Внутренние интерфейсы плат.  Интерфейсы удаленного администрирования. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 3. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 4. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 5. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); |
| БД с ПДн  Служебная БД | Внутренние интерфейсы плат.  Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 3. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 4. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); |
| Веб сервер | Внутренние интерфейсы плат.  Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 3. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 4. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); |
| АРМ работников | Внутренние интерфейсы. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 3. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 4. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 5. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ.  Категория:  Внутренний Н2 | Cisco 2811  Cisco 2960 | Внутренние интерфейсы плат.  Интерфейсы удаленного администрирования. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); 7. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| БД с ПДн  Служебная БД | Внутренние интерфейсы плат.  Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); 7. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| Веб сервер | Внутренние интерфейсы плат.  Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); 7. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| АРМ работников | Внутренние интерфейсы. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию); 7. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)  Категория:  Внутренний Н1 | Cisco 2811  Cisco 2960 | Внутренние интерфейсы плат.  Интерфейсы удаленного администрирования. | 1. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| БД с ПДн  Служебная БД | Внутренние интерфейсы плат.  Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| Веб сервер | Внутренние интерфейсы плат.  Интерфейс пользователя веб-сайта. | 1. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| АРМ работников | Внутренние интерфейсы. | 1. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| Авторизованные пользователи систем и сетей  Категория:  Внутренний Н1 | Веб сервер | Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 5. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| АРМ работников | Внутренние интерфейсы плат. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 5. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| Системные администраторы и администраторы безопасности  Категория:  Внутренний Н2 | Cisco 2811  Cisco 2960 | Внутренние интерфейсы плат.  Интерфейсы удаленного администрирования. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| БД с ПДн  Служебная БД | Внутренние интерфейсы плат.  Пользовательский веб-интерфейс доступа к базе данных информационной системы  Интерфейс общения БД с другими компонентами сети: 1433 порт MSSQL | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| Веб сервер | Внутренние интерфейсы плат.  Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| АРМ работников | Внутренние интерфейсы. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); 2. внедрение вредоносного программного обеспечения; 3. установка программных и (или) программно-аппаратных закладок  в программное обеспечение и (или) программно-аппаратные средства; 4. формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных; 5. инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации; 6. ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств. |
| Бывшие работники  Категория:  Внешний Н1 | Веб сервер | Интерфейс пользователя веб-сайта. | 1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей,  а также организационных и многофакторных уязвимостей); |

Потенциальные УБИ

|  |  |
| --- | --- |
| Преступные группы (криминальные структуры), внешний Н2 | УБИ. 003 Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации  УБИ. 005 Угроза внедрения вредоносного кода в BIOS УБИ. 006 Угроза внедрения кода или данных  УБИ. 007 Угроза воздействия на программы с высокими привилегиями  УБИ. 008 Угроза восстановления и/или повторного использования аутентификационной информации  УБИ. 012 Угроза деструктивного изменения конфигурации/среды окружения программ УБИ. 013 Угроза деструктивного использования декларированного функционала BIOS УБИ. 015 Угроза доступа к защищаемым файлам с использованием обходного пути УБИ. 016 Угроза доступа к локальным файлам сервера при помощи URL УБИ. 017 Угроза доступа/перехвата/изменения HTTP cookies УБИ. 019 Угроза заражения DNS-кеша УБИ. 022 Угроза избыточного выделения оперативной памяти  УБИ. 023 Угроза изменения компонентов информационной (автоматизированной) системы  УБИ. 025 Угроза изменения системных и глобальных переменных  УБИ. 027 Угроза искажения вводимой и выводимой на периферийные устройства информации  УБИ. 028 Угроза использования альтернативных путей доступа к ресурсам  УБИ. 030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию  УБИ. 031 Угроза использования механизмов авторизации для повышения привилегий  УБИ. 032 Угроза использования поддельных цифровых подписей BIOS  УБИ. 033 Угроза использования слабостей кодирования входных данных  УБИ. 034 Угроза использования слабостей протоколов сетевого/локального обмена данными  УБИ. 035 Угроза использования слабых криптографических алгоритмов BIOS  УБИ. 036 Угроза исследования механизмов работы программы  УБИ. 037 Угроза исследования приложения через отчёты об ошибках  УБИ. 041 Угроза межсайтового скриптинга  УБИ. 042 Угроза межсайтовой подделки запроса  УБИ. 045 Угроза нарушения изоляции среды исполнения BIOS  УБИ. 046 Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия  УБИ. 049 Угроза нарушения целостности данных кеша  УБИ. 053 Угроза невозможности управления правами пользователей BIOS  УБИ. 067 Угроза неправомерного ознакомления с защищаемой информацией  УБИ. 068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением  УБИ. 069 Угроза неправомерных действий в каналах связи  УБИ. 071 Угроза несанкционированного восстановления удалённой защищаемой информации  УБИ. 072 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS  УБИ. 073 Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети  УБИ. 074 Угроза несанкционированного доступа к аутентификационной информации  УБИ. 080 Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической  УБИ. 082 Угроза несанкционированного доступа к сегментам вычислительного поля  УБИ. 083 Угроза несанкционированного доступа к системе по беспроводным каналам  УБИ. 084 Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети  УБИ. 085 Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации  УБИ. 086 Угроза несанкционированного изменения аутентификационной информации  УБИ. 087 Угроза несанкционированного использования привилегированных функций BIOS  УБИ. 088 Угроза несанкционированного копирования защищаемой информации  УБИ. 089 Угроза несанкционированного редактирования реестра  УБИ. 090 Угроза несанкционированного создания учётной записи пользователя  УБИ. 091 Угроза несанкционированного удаления защищаемой информации  УБИ. 092 Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам  УБИ. 093 Угроза несанкционированного управления буфером  УБИ. 094 Угроза несанкционированного управления синхронизацией и состоянием  УБИ. 095 Угроза несанкционированного управления указателями  УБИ. 098 Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб  УБИ. 099 Угроза обнаружения хостов  УБИ. 100 Угроза обхода некорректно настроенных механизмов аутентификации УБИ. 102 Угроза опосредованного управления группой программ через совместно используемые данные УБИ. 103 Угроза определения типов объектов защиты УБИ. 104 Угроза определения топологии вычислительной сети УБИ. 109 Угроза перебора всех настроек и параметров приложения УБИ. 111 Угроза передачи данных по скрытым каналам УБИ. 113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники УБИ. 114 Угроза переполнения целочисленных переменных УБИ. 115 Угроза перехвата вводимой и выводимой на периферийные устройства информации УБИ. 116 Угроза перехвата данных, передаваемых по вычислительной сети УБИ. 117 Угроза перехвата привилегированного потока  УБИ. 118 Угроза перехвата привилегированного процесса УБИ. 119 Угроза перехвата управления гипервизором УБИ. 121 Угроза повреждения системного реестра |
| Отдельные физические лица (хакеры) | УБИ. 006 Угроза внедрения кода или данных |
| Конкурирующие организации |  |
| Разработчики программных, программно-аппаратных средств |  |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем |  |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | УБИ. 004 Угроза аппаратного сброса пароля BIOS УБИ. 005 Угроза внедрения вредоносного кода в BIOS  УБИ. 006 Угроза внедрения кода или данных  УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | УБИ. 004 Угроза аппаратного сброса пароля BIOS УБИ. 005 Угроза внедрения вредоносного кода в BIOS  УБИ. 006 Угроза внедрения кода или данных  УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS |
| Авторизованные пользователи систем и сетей | УБИ. 004 Угроза аппаратного сброса пароля BIOS УБИ. 005 Угроза внедрения вредоносного кода в BIOS  УБИ. 006 Угроза внедрения кода или данных  УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS УБИ. 008 Угроза восстановления и/или повторного использования аутентификационной информации |
| Системные администраторы и администраторы безопасности | УБИ. 004 Угроза аппаратного сброса пароля BIOS УБИ. 005 Угроза внедрения вредоносного кода в BIOS  УБИ. 009 Угроза восстановления предыдущей уязвимой версии BIOS УБИ. 007 Угроза воздействия на программы с высокими привилегиями  УБИ. 008 Угроза восстановления и/или повторного использования аутентификационной информации |
| Бывшие работники | УБИ. 008 Угроза восстановления и/или повторного использования аутентификационной информации |