УТВЕРЖДАЮ

Руководитель

И. О. Фамилия

«___» _____ 2024 г.

Приложение 3 к Методике …

Модель угроз безопасности информации

2024

Содержание

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
АС – автоматизированная система
АСЗИ – автоматизированная система в защищенном исполнении
ГАС – государственная информационная система
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
ОС – операционная система
ПМВ – программно–математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗ – система (подсистема) защиты
СКЗИ – средства криптографической защиты информации
СОВ – система обнаружения вторжений
ТС – техническое средство
УБ – угрозы безопасности

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система (АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) — программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Архитектура — совокупность основных структурно-функциональных характеристик, свойств, компонентов, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при ее обработке в информационных системах.

Взаимодействующая (смежная) система — система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с другой системой или сетью, и не включена оператором системы или сети в границы процесса оценки угроз безопасности информации.

Вирус (компьютерный, программный) — исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Возможности нарушителя — мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

Вредоносная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Вспомогательные технические средства и системы (ВТСС) — технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информация — данные, содержащиеся в системах и сетях (в том числе защищаемая информация, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.).

Информационная система (ПС) — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть (ИТКС) — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные ресурсы — информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

Компонент — программное, программно-аппаратное или техническое средство, входящее в состав системы.

Контролируемая зона — пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Недокументированные (недекларированные) возможности — функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ, несанкционированные действия — доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Обеспечивающие системы инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

Обработка информации — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение; уточнение (обновление, изменение), извлечение; использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Основные (критические) процессы (бизнес-процессы) — управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные излучения технических средств обработки защищаемой информации,

возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также

электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь — лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка — скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программно-аппаратное средство — устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

Программное обеспечение – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Сеть электросвязи — сеть связи, предназначенная для электросвязи (передача и прием сигналов, отображающих звуки, изображения, письменный текст, знаки или сообщения любого рода по электромагнитным системам).

Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗП) — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средство защиты информации (СЗИ) — техническое, программное,

программно-техническое средство, вещество и (или) материал предназначенные или используемые для защиты информации.

Средства вычислительной техники (СВТ) — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технический канал утечки информации (ТКЗИ) — совокупность носителя информации (средства обработки), физической среды распространения информативною сигнала и средств, которыми добывается защищаемая информация.

Угроза безопасности информации (УБИ) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

Утечка (защищаемой) информации по техническим каналам — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость — недостаток (слабость) программною (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

1 Общие положения

Настоящая модель угроз безопасности информации (далее - Модель угроз) содержит результаты оценки угроз безопасности информации комплекса Телеком-Техно.

1.1 Назначение и область действия документа

Модель угроз предназначена для определения угроз безопасности информации, реализация (возникновение) которых возможна в автоматизированной системе (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой в АС информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования АС, актуальных угроз безопасности информации.

Модель угроз распространяется на комплекс Телеком-Техно.

Настоящая Модель угроз может быть пересмотрена:

– по решению владельца АС на основе периодически проводимых анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений АС;

– в случае возникновения (обнаружения) новых уязвимостей и угроз безопасности информации;

– в случае изменения федерального законодательства в части оценки угроз безопасности информации;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности информации;

– в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования АС;

– в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;

– в случаях выявления инцидентов информационной безопасности в АС и (или) взаимодействующих (смежных) системах.

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

Настоящая Модель угроз сформирована в соответствии с методическими документами ФСТЭК России и ФСБ России с учетом следующих принципов:

– в случае обеспечения безопасности информации без использования СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России;

– в случае необходимости обеспечения безопасности информации с использованием СКЗИ при формировании Модели угроз используются методические документы ФСБ России и ФСТЭК России.

Перечень нормативных правовых актов, методических документов и национальных стандартов, используемый для оценки угроз безопасности информации и разработки Модели угроз, представлен в Приложении № 1.

1.3 Наименование обладателя информации, заказчика, оператора систем и сетей

Информация об организациях, имеющих отношение к АС, представлена в таблице 1.2.

Таблица 1.2 - Перечень организаций

№ п/п	Роль организации	Организация
1	Обладатель информации	ООО «Техно-Телеком»
2	Заказчик	ООО «Техно-Телеком»
3	Разработчик изделия	ООО «Техно-Телеком»

1.4 Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей

Ответственные за защиту информации, содержащейся в АС, назначаются должностные лица/подразделения приказом командира войсковой части, в эксплуатацию которого передано изделие Телеком-Техно.

Ответственные за обеспечение защиты информации (безопасности) представлены в таблице 1.3.

Таблица 1.3 - Ответственные за обеспечение защиты информации (безопасности)

№ п/п	Роль подразделения/ должностного лица	Должностное лицо / подразделение
1	Ответственный за защиту информации, содержащей сведения, составляющие государственную тайну	Орган ЗГТ В/Ч № …
2	Ответственный за планирование и контроль мероприятий по обеспечению информационной безопасности	
3	Ответственный за управление (администрирование) системой защиты информации (подсистемой безопасности)	
4	Ответственный за выявление компьютерных инцидентов и реагирование на них	
5	Сотрудник, которому разрешены действия по внесению изменений в конфигурацию	

1.5 Наименование организации, привлекаемой для разработки модели угроз безопасности информации

Разработка модели угроз безопасности информации осуществлялась ООО «Безопасность-Техно».

2 Описание систем и сетей и их характеристика как объектов защиты

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

Модель угроз разработана для изделия Телеком-Техно, в состав которого входят:

– менее четырех ЭВМ;

– наземный пункт управления;

– наземный модуль связи.

2.2 Класс защищенности, категория значимости систем и сетей, уровень защищенности

В соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссии России 1992 г.) составные части изделия Телеком-Техно имеют следующие классы защищенности информации от несанкционированного доступа:

– АС наземного модуля связи – класс 1В защищенности информации от несанкционированного доступа (многопользовательская с разными правами);

– АС наземного модуля управления – класс 1В защищенности информации от несанкционированного доступа (многопользовательская с разными правами);

– АС ЭВМ – класс 1В защищенности информации от несанкционированного доступа (многопользовательская с разными правами);

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

Изделие Телеком-Техно создается в соответствии с тактико-техническим заданием на опытно-конструкторскую работу «Телеком-Техно»).

Функционирование изделие осуществляется в соответствии с эксплуатационной документацией на изделие Телеком-Техно.

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

Телеком-Техно предназначен для ведения секретной деятельности.

Наземный пункт управления Телеком-Техно предназначен для выполнения следующих задач:

– автоматизация процессов ведения секретной деятельности;

– управление функционированием Телеком-Техно в целом.

Наземный пункт связи предназначен для выполнения следующих задач:

– дистанционного управления ЭВМ;

– приема, обработки и хранения секретных сведений.

Состав обрабатываемой информации и ее правовой режим указан в документе «Перечень информации, циркулирующей в Телеком-Техно».

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

Основным процессом обладателя информации и операторов является ведение секретной деятельности.

Основные процессы в Телеком-Техно:

– получение секретных сведений;

– определение возможностей противника;

– разработка планов и историй;

– разработка план-графика планов.

Основные процессы оператора Телеком-Техно:

– анализ секретных сведений;

– получение информация о возможностях противника;

– расчет потребного план-графика планов;

– уточнение маршрута историй.

Основные процессы администратора безопасности информации:

– настройка средств защиты информации;

– блокирование/разблокирование работы пользователя, программ и устройств ПТК в случае обнаружения попыток, фактов НСД;

– просмотр и печать (при необходимости) АБИ журналов подсистемы регистрации и учёта;

– архивацию журналов регистрации за необходимый промежуток времени;

– ведение журнала учёта защищаемых ресурсов (каталогов, файлов, программ);

– ведение таблицы разграничения доступа (с возможностью документирования) пользователей, их прав, полномочий;

– корректировку параметров идентификации и полномочий доступа к защищаемым ресурсам;

– генерацию, установку и смену паролей доступа пользователям использованием программы генерации пароля;

– формирование и печать списка пользователей с соответствующими им заблаговременно сгенерированными паролями;

– отображение и документирование результатов контроля целостности программного обеспечения;

– проведение антивирусной проверки средств вычислительной техники;

– отображение и документирование результатов антивирусной проверки ПО с указанием элементов подвергшихся заражению;

– создание резервных копий действующих параметров средств защиты информации, а также рабочих копий машинных носителей информации;

– тестирование работоспособности средств защиты информации.

Основные процессы инженера связи:

– проверка состояния связи;

– анализ распоряжений по организации связи Телеком-Техно.

Основные процессы техника станции:

– обеспечение работоспособности оборудования;

– включение-выключение пункта управления;

– проведение регламентных работ в пункте управления, ведение формуляров;

– анализ телеметрии, наблюдение за состоянием оборудования по ключевым параметрам;

– проведение оперативного восстановления работоспособности пункта управления в случае возникновения сбоев и отказов;

– ведение журнала отказов и сбоев, сбор статистики.

Основные процессы оператора Телеком-Техно:

– выбор типа подготовки для контроля;

– выбор системы объекта контроля;

– ввод исходных данных (на определённых операциях контроля);

– наблюдение за индикацией (окнами на экране ПЭВМ);

– распознавание результатов контроля, принятие решение.

Основными процессами разработчика изделия является проектирование, изготовление и испытание изделия на различных этапах жизненного цикла, его модернизация и ремонт.

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

В состав Телеком-Техно включены:

– не менее четырех ЭВМ;

– наземный пункт управления;

– наземный модуль связи.

Состав программных и программно-аппаратных средств автоматизированной системы представлен в таблице 2.1.

Таблица 2.1 — Состав АС

№ п/п	Характеристика	Значение характеристики
1	Программно-аппаратные средства	Телеком-Техно-Программы
2	Общесистемное ПО	ОС СН «Astra Linux Special Edition»
3	Прикладное ПО	СПО
4	СЗИ	ОС СН «Astra Linux Special Edition» САВЗ Dr.Web Enterprise Security Suite ПАК «Dionis-NX» СЗД «Dallas Lock»

АС представляют собой распределенную систему (комплекс автоматизированных рабочих мест, коммуникационною и серверного оборудования).

2.7 Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа

Пользователи систем и сетей Телеком-Техно входят в составные части.

Группам пользователей присваиваются следующие виды доступа: R - чтение, W - запись, X - чтение и исполнение, M - изменение, F - поиск; «+» - вид доступа разрешен, «-» - вид доступа запрещен.

Наземный пункт управления предназначен для размещения и обеспечения выполнения функционала, следующих должностных лиц:

- руководитель расчета;
- администратор безопасности информации;
- инженер связи;
- техник станции.

Группы пользователей систем и сетей, уровней их полномочий и типов доступа автоматизированной системы элементов НП пункта управления представлены в таблицах 2.2 и 2.3.

Таблица 2.3. Права доступа к автоматизированным рабочим местам НП пункта управления

№ п/п	Группы	АРМ НП пункта управления				
		Разрешенные Каталоги/файлы	Принтер	Устройство чтения оптических дисков, ЗМНИ	Базовая система ввода-вывода (BIOS)	Загрузчик ОС (grub)
1	Руководитель расчета	R, W, X, F	R, W	R, W, F-	-	-
2	Инженер связи	R, X, F	-	-	-	-
3	Техник станции	-	-	-	-	-
4	Администратор безопасности информации	R, M, X, W, F	R, M, X, W, F	R, M, W, F	-	R, M, W

Таблица 2.3. Права доступа к серверам НП пункта управления

№ п/п	Группы	Серверы НП пункта управления				
		Разрешенные Каталоги/файлы	**Принтер**	**Устройство чтения оптических дисков, ЗМНИ**	**Базовая система ввода-вывода (BIOS)**	**Загрузчик ОС (grub)**
1	Руководитель расчета	-	-	-	-	-
2	Инженер связи	-	-	-	-	-
3	Техник станции	-	-	-	-	-
4	Администратор безопасности информации	R, M, X, W, F	R, M, X, W, F	R, M, W, F	-	R, M, W

Таблица 2.4. Права доступа к автоматизированным рабочим местам НМ пункта управления

№ п/п	Группы	АРМ				
		Разрешенные Каталоги/файлы	**Принтер**	**Устройство чтения оптических дисков, ЗМНИ**	**Базовая система ввода-вывода (BIOS)**	**Загрузчик ОС (grub)**
1	Руководитель расчета	R, W, X, F	R, W	R, W, F-	-	-
2	Инженер связи	R, X, F	-	-	-	-
3	Техник станции	-	-	-	-	-
4	Администратор безопасности информации	R, M, X, W, F	R, M, X, W, F	R, M, W, F	-	R, M, W

2.8 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»

Внешние интерфейсы и взаимодействие составных частей Телеком-Техно с пользователями, иными системами и сетями, обеспечивающими системами представлены в КД, взаимодействие внутри отдельных составных частей приведено в КД.

К информационным ресурсам АС осуществляется локальный и удаленный доступ.

Подключение к информационно-телекоммуникационным сетям и сети «Интернет» – отсутствует.

В АС осуществляется взаимодействие с другими системами комплексов средств автоматизации.

При функционировании Телеком-Техно используются следующие технологии:

- съемные носители информации;
- технологии беспроводного доступа;
- технология передачи видеоинформации;
- технология удаленного администрирования;
- технология удаленного внеполосного доступа;
- технология передачи речи;
- технология искусственного интеллекта.

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

В ходе оценки угроз безопасности информации определяются негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

Описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов представлены в таблице 3.1.

Негативные последствия определялись применительно к нарушению основных (критических) процессов, выполнение которых обеспечивает АС, и применительно к нарушению безопасности информации, содержащейся в АС.

Соответствие возможных целей реализации угроз безопасности информации с негативными последствиями представлено в Приложении 2.

Описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба) представлены в таблице 3.1.

На основе анализа исходных данных АС определены негативные последствия, которые приводят к видам рисков (ущерба), представленные в таблице 3.1.

Таблица 3.1 Таблица — Виды рисков (ущерба) и негативные последствия

Идентификатор	Негативные последствия	Виды риска (ущерба)
НП.1	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов	У3. Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности
НП.2	Утечка информации ограниченного доступа	

4 Возможные объекты воздействия угроз безопасности информации

Наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемой информации, или обеспечивают реализацию основных процессов обладателя информации, оператора представлены в п. 2.4 настоящей Модели угроз.

Объекты воздействия определялись для реальной архитектуры и условий функционирования АС на основе анализа исходных данных.

Определение объектов воздействия производилось на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.

В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям.

Описание видов воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям представлены в таблице 4.1.

Таблица 4.1 Таблица — Виды воздействия

Идентификатор	Вид воздействия
ВВ.1	утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.5	несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач
ВВ.6	нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

Итоговый перечень объектов воздействия со списком возможных видов воздействия на них, реализация которых может привести к негативным последствиям, представлен в таблице 4.2.

Таблица 4.2 Таблица — Объекты воздействия и виды воздействия

Негативные последствия	Объекты воздействия	Виды воздействия
Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов.	BIOS/UEFI	ВВ.2, ВВ.3, ВВ.4
	Сетевое оборудование	ВВ.2, ВВ.3, ВВ.4, ВВ.6
	Сетевое ПО	ВВ.2, ВВ.3, ВВ.4
	Сетевой трафик	ВВ.1, ВВ.2, ВВ.4
	Прикладное ПО	ВВ.2, ВВ.3, ВВ.4
	База данных	ВВ.1, ВВ.2, ВВ.4
	Защищаемая информация	ВВ.1, ВВ.2, ВВ.4
	Системное ПО	ВВ.2, ВВ.3, ВВ.4
	Средство вычислительной техники	ВВ.1, ВВ.2, ВВ.3, ВВ.4, ВВ.5, ВВ.6
	СЗИ	ВВ.2, ВВ.3, ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы)	ВВ.2, ВВ.3, ВВ.4, ВВ.6
	Информационная (автоматизированная) система	ВВ.1, ВВ.2, ВВ.3, ВВ.4, ВВ.5, ВВ.6
	Машинный носитель информации в составе СВТ	ВВ.1, ВВ.2, ВВ.3, ВВ.4
	Микропрограммное обеспечение	ВВ.2, ВВ.3, ВВ.4
	Учетные данные пользователей	ВВ.1, ВВ.2, ВВ.4
	Прикладное ПО	ВВ.2, ВВ.3, ВВ.4
	Система поддержания температурно-влажностного режима	ВВ.2, ВВ.3, ВВ.4
Утечка информации ограниченного доступа	BIOS/UEFI	ВВ.2, ВВ.3, ВВ.4
	Сетевое оборудование	ВВ.2, ВВ.3, ВВ.4, ВВ.6
	Сетевое ПО	ВВ.2, ВВ.3, ВВ.4
	Сетевой трафик	ВВ.1, ВВ.2, ВВ.4
	База данных	ВВ.1, ВВ.2, ВВ.4
	Системное ПО	ВВ.2, ВВ.3, ВВ.4
	Средство вычислительной техники	ВВ.1, ВВ.2, ВВ.3, ВВ.4, ВВ.5, ВВ.6
	СЗИ	ВВ.2, ВВ.3, ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы)	ВВ.2, ВВ.3, ВВ.4, ВВ.6
	Защищаемая информация	ВВ.1, ВВ.2, ВВ.4
	Машинный носитель информации в составе СВТ	ВВ.1, ВВ.2, ВВ.3, ВВ.4
	Микропрограммное обеспечение	ВВ.2, ВВ.3, ВВ.4
	Учетные данные пользователей	ВВ.1, ВВ.2, ВВ.4
	Объекты файловой системы	ВВ.1, ВВ.2, ВВ.4
	Прикладное ПО	ВВ.2, ВВ.3, ВВ.4

5 Модель нарушителя

5.1 Характеристики нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации

В ходе оценки угроз безопасности информации определены возможные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие(ая) реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты АС, актуальные нарушители.

Процесс определения актуальных нарушителей включает формирование перечня рассматриваемых видов нарушителей и их возможных целей по реализации угроз безопасности информации и предположений об их отнесении к числу возможных нарушителей (нарушителей, подлежащих дальнейшей оценке).

Характеристики нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации представлены в таблицы 5.1.

Таблица 5.1 — Перечень рассматриваемых нарушителей

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
1.	Специальные службы иностранных государств	Нанесение ущерба государству в области обороны безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики; Дискредитация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства; Создание внутриполитического кризиса.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
2.	Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан; Нанесение ущерба отдельным сферам деятельности или секторам экономики государства; Дестабилизация общества; Дестабилизация деятельности органов государственной власти, организаций.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
3.	Преступные группы (криминальные структуры)	Получение финансовой или иной материальной выгоды; Желание самореализации (подтверждение статуса).	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
4.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса).	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
5.	Конкурирующие организации	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
6.	Разработчики программных, программно-аппаратных средств	Получение финансовой или иной маной выгоды; Получение конкурентных преимуществ; Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки; Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
8.	Поставщики вычислительных услуг, услуг связи	Получение финансовой иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
9.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
10.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой иной материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
11.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
12.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
13.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды; Месть за ранее совершенные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

5.2 Категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации

В ходе анализа потенциала категории актуальных нарушителей, требуемого для использования уязвимости, необходимо учитывать следующие факторы:

– время, затрачиваемое на идентификацию уязвимости;

– время, затрачиваемое на использование уязвимости;

– техническая компетентность нарушителя;

– знание проекта и функционирования системы;

– аппаратные средства, программное обеспечение или другое оборудование, доступное нарушителю.

Уровни возможностей нарушителей представлены в Приложении 3.

Учитывая комплекс режимных мер, направленных на отбор технического персонала (5-7 вид нарушителя, таблица 5.1), данная категория физических лиц, имеющих санкционированный доступ к АС и реализацию возможности нарушителей рассматриваем как низкую.

Кроме того, исходя из комплекса режимных и организационно-технических мер, действующих внутри контролируемой зоны, не детализируются угрозы информационной безопасности в АС, источником которых являются возможные преднамеренные действия физических лиц, имеющих доступ внутрь контролируемой зоны, но не имеющих санкционированного доступа к АС (4 вид нарушителя, таблица 5.1).

Нарушитель, имеющий доступ к техническим и программным средствам АС, но не являющийся зарегистрированным пользователем или техническим персоналом (3 и 4 вид нарушителя, таблица 5.1) с целью удовлетворения любопытства, самоутверждения, получения возможной материальной выгоды и т.п. может осуществлять преднамеренные действия по НСД к подлежащим защите объектам, используя оставленные без контроля автоматизированные рабочие места (их штатные программно-технические средства), другие технические средства, носители конфиденциальной информации и т.д. При этом нарушитель может осуществлять манипуляции с органами управления автоматизированных рабочих мест из состава

Изделия с использованием только штатных средств без нарушения их целостности и будет предпринимать действия по сокрытию попыток НСД.

С точки зрения конфиденциальности реализацию возможности внешнего нарушителя (1 и 2 вид нарушителя, таблица 5.1) рассматриваем как низкую, так как информация, выходящая за пределы контролируемой зоны, передается только по каналам связи с использованием сертифицированных шифровальных средств и может представлять интерес для реализации возможности нарушителя и к тому же учитывая высокую стоимость и сложность подготовки и реализации этой возможности. Однако внешний нарушитель может попытаться получить сведения о сетевой структуре АС, используя сетевые технологии или нарушить доступность взаимодействия компонентов АС, через неконтролируемую зону.

5.3 Описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

Сопоставление возможных нарушителей, их целей реализации угроз безопасности информации с возможными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз безопасности информации, а также описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей представлены в таблице 5.2.

Таблица 5.2 — Характеристики возможных нарушителей

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
1.	Отдельные физические лица (хакеры)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
3.	Поставщики вычислительных услуг, услуг связи	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
	оператора			
6.	Авторизованные пользователи систем и сетей	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да
7.	Системные администраторы и администраторы безопасности	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
8.	Бывшие (уволенные) работники (пользователи)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Нет

6 Способы реализации (возникновения) угроз безопасности информации

В ходе оценки угроз безопасности информации определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в АС - актуальные способы реализации (возникновения) угроз безопасности информации.

Перечень исключенных из базового перечня угроз безопасности информации представлен в Приложении 4.

Перечень возможных способов реализации угроз безопасности информации представлен в таблице 6.1.

Таблица 6.1 — Перечень возможных способов реализации угроз безопасности информации

Идентификатор	Способы реализации
СР.1	Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)
СР.2	Внедрение вредоносного ПО
СР.3	Использование недекларированных возможностей ПО и (или) программно-аппаратных средств
СР.4	Установка программных и (или) программно-аппаратных закладок в ПО (или) программно-аппаратные средства
СР.5	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных
СР.6	Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.7	Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установки, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию)
СР.8	Ошибочные действия в ходе создания и эксплуатации сетей и систем, в том числе при установке, настройке программных и программно-аппаратных средств
СР.9	Перехват трафика сети передачи данных
СР.10	Несанкционированный физический доступ и (или) воздействие на линии (каналы) связи, технические средства, машинные носители информации
СР.11	Реализация атак типа «отказ в обслуживании» в отношении технических средств, программного обеспечения и каналов передачи данных

Определение интерфейсов объектов воздействия, определенных в соответствии с разделом 2.8 настоящей Модели угроз. Интерфейсы объектов воздействия определялись на основе изучения и анализа данных:

- об архитектуре, составе и условиях функционирования АС;
- о группах пользователей АС, их типов доступа и уровней полномочий.

Результаты процесса определения актуальных способов реализации (возникновения) угроз безопасности информации, включающие описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы актуальными нарушителями, и описание интерфейсов объектов воздействия, доступных для использования актуальным нарушителям, представлены в таблице 6.2.

Таблица 6.2 - Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

Вид нарушителя	**Категория нарушителя**	**Объекты воздействия**	**Доступные интерфейсы**	**Способы реализации (идентификатор)**
1	**2**	**3**	**4**	**5**
Отдельные физические лица (хакеры)	Внешний	Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.11
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.8, СР.11
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.8, СР.9, СР.11
		Системное программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.2
		Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.2
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.8, СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.2, СР .11
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.9
		Информационная (автоматизированная) система	Пользователи	СР.1
		Учетные данные пользователя	Каналы связи с внешними информационно-	СР.9

1	2	3	4	5
			телекоммуникационными сетями	
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.4, СР.9
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1, СР.3, СР.8
			Физический доступ к аппаратному обеспечению BIOS	СР.7, СР.8, СР.10
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.4, СР. 5, СР 7, СР .8, СР.10
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.7, СР.8, СР.10
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защита информации	СР.1, СР.8
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.7, СР.10
		Защищаемая информация	Доступ через средства вычислительной техники	СР.1, СР.4, СР.8, СР.10
Поставщики вычислительных услуг, услуг связи	Внутренний	Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.11
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.8, СР.11
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.8, СР.9, СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1, СР.2, СР.11
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.9
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.9

1	2	3	4	5
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР 1, СР.4, СР.8
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1, СР.3, СР.8
			Физический доступ к аппаратному обеспечению BIOS	СР.7, СР.8, СР.10
			Механизм обновления BIOS/UEFI	СР.1, СР.2, СР.8
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.4, СР.5, СР. 7, СР.8, СР.10
		Сетевое программное обеспечение	Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР.5, СР.7, СР.8
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1, СР.8, СР.9, СР.11
		База данных	Пользовательский интерфейс СУБД	СР.8
			Служебные программы командной строки СУБД	СР.8
		Системное программное обеспечение	Доступ через средства вычислительной техники	СР.1, СР.2, СР.3, СР.4, СР.7, СР.8
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.7, СР.8, СР.10
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1, СР.2, СР.8
			Интерфейсы подключения съемных машинных носителей информации	СР.1, СР.2
		Средство защиты информации	Доступ через средства вычислительной техники	СР.1, СР.8
			Физический доступ к программно-аппаратным средствам защиты информации	СР.7, СР.10
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.7, СР.10
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2, СР.8
		Защищаемая информация	Доступ через средства вычислительной техники	СР.1, СР.4, СР.8, СР10
			Физический доступ к программно-аппаратным средствам обработки	СР.6, СР.10

1	2	3	4	5
			информации	
		Информационная (автоматизированная) система	Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.8
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.7, СР .8
			Физический доступ к машинным носителям информации	СР.10
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.7
		Съемный машинный носитель информации	Через функции ввода-вывода низкого уровня (прямого доступа)	СР.7
			Физический доступ к съемным машинным носителям информации	СР.10
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1, СР.3, СР.8
			Механизм обновления микропрограммного обеспечения	СР.2, СР.4
		Учетные данные пользователя	Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1, СР.8
		Прикладное программное обеспечение	Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР.7, СР.8
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1, СР.3, СР.8
			Физический доступ к аппаратному обеспечению BIOS	СР.7, СР.8, СР.10
			Механизм обновления BIOS/UEFI	СР.1, СР.2, СР.8
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.4, СР.5, СР.7, СР.8, СР.10
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.7, СР.8, СР.10
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защиты информации	СР.7, СР.10
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.7, СР.10

1	2	3	4	5
		Защищаемая информация	Физический доступ к программно-аппаратным средствам обработки информации	СР.6, СР.10
		Машинный носитель информации в составе средств вычислительной техники	Физический доступ к машинным носителям информации	СР.10
		Съемный машинный носитель информации	Физический доступ к съемным машинным носителям информации	СР.10
		Объекты файловой системы	Физический доступ к машинным носителям информации	СР.1, СР.4, СР.7, СР.10
Авторизованные пользователи систем и сетей	Внутренний	BIOS/UEFI	Физический доступ к аппаратному обеспечению BIOS	СР.7, СР.8, СР.10.
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1, СР.11
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1, СР.8, СР.11
			Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР 5, СР.7, СР.8
		База данных	Прикладное приложение, использующее базу данных	СР.1
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1, СР.2
			Доступ через средства вычислительной техники	СР.1, СР.2, СР.3, СР.4, СР.7, СР.8
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1, СР.2
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.7, СР.8, СР.10
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1, СР 2, СР 8
			Интерфейсы подключения съемных машинных носителей-	СР.1, СР.2
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1, СР.11
			Доступ через средства вычислительной техники	СР.10, СР.8
			Физический доступ к программно-аппаратным средствам защиты ин формации	СР.7, СР.10
		Узел вычислительной сети	Каналы связи узлов локальной вычислительной	СР.1, СР.2, СР.11

1	2	3	4	5
		(автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы и т.п.)	сети	
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7, СР.10
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2, СР.8
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.9
			Доступ через средства вычислительной техники	СР.1, СР.4, СР.8, СР.10
			Физический доступ к программно-аппаратным средствам обработки информации	СР.6, СР.10
		Машинный носитель информации	Доступ через средства вычислительной техники	СР.7, СР.8
		в составе средств вычислительной техники	Физический доступ к машинным носителям информации	СР.10
		Съемный машинный носитель информации	Физический доступ к съемным машинным носителям информации	СР.10
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1, СР.3, СР.8
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.9
			Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1, СР.8
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1, СР.4, СР.8
			Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР.7, СР.8
			Физический доступ к машинным носителям информации	СР.1, СР.4, СР.7, СР.10
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1, СР.11
			Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР.7, СР.8
Системные администраторы и администраторы безопасности	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1, СР.7
			Физический доступ к аппаратному обеспечению BIOS	СР.6, СР.7, СР.9
			Механизм обновления	СР.1, СР.2, СР.7

1	2	3	4	5
			BIOS/UEFI	
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1, СР.10
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.4, СР.5, СР.7, СР.8, СР.10
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1, СР.8, СР.11
			Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР.5, СР.7, СР.8
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1, СР.8, СР.9, СР.11
		База данных	Пользовательский интерфейс СУБД	СР.8
			Служебные программы командной строки СУБД	СР.8
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1, СР.2
			Доступ через средства вычислительной техники	СР.1, СР.2, СР.3, СР.4, СР.7, СР.8
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1, СР.2
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3, СР.7, СР.8, СР.12
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1, СР.2, СР.8
			Интерфейсы подключения съемных машинных носителей информации	СР.1, СР.2
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1, СР.8, СР.11
			Доступ через средства вычислительной техники	СР.1, СР.8
			Физический доступ к программно-аппаратным средствам защиты информации	СР.7, СР.10
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы и т.п.)	Каналы связи узлов локальной вычислительной сети	СР.1, СР.2, СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7, СР.10

1	2	3	4	5
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2, СР.8
			Каналы удаленного администрирования узла вычислительной сети	СР.1
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.9
			Доступ через средства вычислительной техники	СР.1, СР.4, СР.8, СР.10
			Физический доступ к программно-аппаратным средствам обработки информации	СР.6, СР.10
		Информационная (автоматизированная) система	Процесс создания (модернизации) информационной (автоматизированной) системы	СР.4, СР.7, СР.8
			Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.8
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.7, СР.8
			Физический доступ к машинным носителям информации	СР.10
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.7
		Съемный машинный носитель информации	Через функции ввода-вывода низкого уровня (прямого доступа	СР.7
			Физический доступ к съемным машинным носителям информации	СР.10
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1, СР.7, СР.8
			Механизм обновления микропрограммного обеспечения	СР.2, СР.4
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.9
			Доступ к объектам файловой системы, содержащим учётные данные пользователя	СР.10, СР.8
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1, СР. 4, СР.8
			Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР.7,

1	2	3	4	5
				СР.8
			Физический доступ к машинным носителям информации	СР.1, СР.4, СР.7, СР.10
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1, СР.10
			Доступ через средства вычислительной техники	СР.1, СР.3, СР.4, СР.7, СР.8

Анализ способов реализации угроз безопасности информации показал, что:

– на этапе создания изделия наиболее актуальными способами реализации угроз будут:

– внедрение вредоносного ПО;

– установка программных и (или) программно-аппаратных закладок в ПО (или) программно-аппаратные средства;

– нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установки, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

– ошибочные действия в ходе создания изделия, в том числе при установке, настройке программных и программно-аппаратных средств;

– несанкционированный физический доступ и (или) воздействие на линии (каналы) связи, технические средства, машинные носители информации.

– на этапе эксплуатации изделия наиболее актуальными угрозами будут:

– формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;

– несанкционированный физический доступ и (или) воздействие на линии (каналы) связи, технические средства, машинные носители информации;

– реализация атак типа «отказ в обслуживании» в отношении технических средств, программного обеспечения и каналов передачи данных;

– перехват трафика сети передачи данных.

7 Актуальные угрозы безопасности информации

В ходе оценки угроз безопасности информации определены возможные угрозы безопасности информации и произведена их оценка на актуальность для АС - актуальные угрозы безопасности информации.

Процесс определения актуальных угроз безопасности информации включал выделение из исходного перечня угроз безопасности информации возможных угроз по следующему принципу: угроза безопасности информации признается возможной, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способ реализации угрозы безопасности информации, и реализация угрозы может привести к негативным последствиям.

В качестве исходного перечня угроз безопасности информации использовался банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru).

Оценку возможных угроз на предмет актуальности по следующему принципу угроза признается актуальной, если имеется хотя бы один сценарий реализации угрозы безопасности информации. Результаты анализа приведены в Приложении 4

Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик приведен в Приложении 5.

Перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации, уровней возможностей нарушителей и описание возможных сценариев реализации угроз безопасности информации приведены в Приложении 6.

По результатам оценки возможных угроз безопасности выявлено 108 актуальных угроз. Итоговый перечень актуальных угроз безопасности информации представлен в таблице 7.1.

Таблица 7.1 — Актуальные угрозы безопасности информации

№ п/п	Идентификатор УБИ	Наименование УБИ
1.	УБИ.004	Угроза аппаратного сброса пароля BIOS
2.	УБИ.006	Угроза внедрения кода или данных
3.	УБИ.007	Угроза воздействия на программы с высокими привилегиями
4.	УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации
5.	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
6.	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
7.	УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
8.	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
9.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
10.	УБИ.018	Угроза загрузки нештатной операционной системы
11.	УБИ.022	Угроза избыточного выделения оперативной памяти
12.	УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
13.	УБИ.025	Угроза изменения системных и глобальных переменных
14.	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
15.	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
16.	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
17.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
18.	УБИ.032	Угроза использования поддельных цифровых подписей BIOS
19.	УБИ.033	Угроза использования слабостей кодирования входных данных
20.	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
21.	УБИ.036	Угроза исследования механизмов работы программы
22.	УБИ.037	Угроза исследования приложения через отчёты об ошибках
23.	УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS
24.	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
25.	УБИ.049	Угроза нарушения целостности данных кеша
26.	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
27.	УБИ.053	Угроза невозможности управления правами пользователей BIOS
28.	УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения
29.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
30.	УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
31.	УБИ.069	Угроза неправомерных действий в каналах связи
32.	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
33.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
34.	УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
35.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
36.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации

№ п/п	Идентификатор УБИ	Наименование УБИ
37.	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
38.	УБИ.088	Угроза несанкционированного копирования защищаемой информации
39.	УБИ.090	Угроза несанкционированного создания учётной записи пользователя
40.	УБИ.091	Угроза несанкционированного удаления защищаемой информации
41.	УБИ.093	Угроза несанкционированного управления буфером
42.	УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
43.	УБИ.095	Угроза несанкционированного управления указателями
44.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
45.	УБИ.099	Угроза обнаружения хостов
46.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
47.	УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
48.	УБИ.103	Угроза определения типов объектов защиты
49.	УБИ.104	Угроза определения топологии вычислительной сети
50.	УБИ.109	Угроза перебора всех настроек и параметров приложения
51.	УБИ.111	Угроза передачи данных по скрытым каналам
52.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
53.	УБИ.114	Угроза переполнения целочисленных переменных
54.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
55.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
56.	УБИ.117	Угроза перехвата привилегированного потока
57.	УБИ.118	Угроза перехвата привилегированного процесса
58.	УБИ.122	Угроза повышения привилегий
59.	УБИ.123	Угроза подбора пароля BIOS
60.	УБИ.124	Угроза подделки записей журнала регистрации событий
61.	УБИ.127	Угроза подмены действия пользователя путём обмана
62.	УБИ.128	Угроза подмены доверенного пользователя
63.	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
64.	УБИ.130	Угроза подмены содержимого сетевых ресурсов
65.	УБИ.131	Угроза подмены субъекта сетевого доступа
66.	УБИ.132	Угроза получения предварительной информации об объекте защиты
67.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
68.	УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
69.	УБИ.144	Угроза программного сброса пароля BIOS
70.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения
71.	УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
72.	УБИ.150	Угроза сбоя процесса обновления BIOS
73.	УБИ.152	Угроза удаления аутентификационной информации
74.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
75.	УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
76.	УБИ.155	Угроза утраты вычислительных ресурсов

№ п/п	Идентификатор УБИ	Наименование УБИ
77.	УБИ.156	Угроза утраты носителей информации
78.	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
79.	УБИ.158	Угроза форматирования носителей информации
80.	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
81.	УБИ.162	Угроза эксплуатации цифровой подписи программного кода
82.	УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций
83.	УБИ.165	Угроза включения в проект не достоверно испытанных компонентов
84.	УБИ.166	Угроза внедрения системной избыточности
85.	УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
86.	УБИ.169	Угроза наличия механизмов разработчика
87.	УБИ.170	Угроза неправомерного шифрования информации
88.	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
89.	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
90.	УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
91.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
92.	УБИ.179	Угроза несанкционированной модификации защищаемой информации
93.	УБИ.182	Угроза физического устаревания аппаратных компонентов
94.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
95.	УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
96.	УБИ.188	Угроза подмены программного обеспечения
97.	УБИ.189	Угроза маскирования действий вредоносного кода
98.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
99.	УБИ.192	Угроза использования уязвимых версий программного обеспечения
100.	УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
101.	УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
102.	УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
103.	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
104.	УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
105.	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
106.	УБИ.212	Угроза перехвата управления информационной системой
107.	УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
108.	УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов

Анализ угроз безопасности информации показал, что:

– на этапе создания изделия наиболее актуальными угрозами будут:

– угроза неправомерного ознакомления с защищаемой информацией осуществляемая внутренним нарушителем;

– угроза подмены доверенного пользователя, осуществляемая внутренним нарушителем;

– угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

– на этапе эксплуатации изделия наиболее актуальными угрозами будут:

– угроза утраты вычислительных ресурсов;

– угроза утраты носителей информации;

– угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

– угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.

Перечисленные угрозы могут быть осуществлены как внутренним, так и внешним нарушителем.

Анализ достаточность принятых мер для нейтрализации угроз безопасности информации с учетом принятой модели нарушителя и способов реализации угроз представлен в Приложении 7.

Приложение 1

Источники, используемые при разработке модели угроз

При разработке модели угроз использовались следующие методические и нормативно-правовые документы и требования:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– «Специальные требования и рекомендации по технической защите информации» (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года №282

– Методический документ «Методика оценки угроз безопасности информации», утвержденный Федеральной службы по техническому и экспортному контролю 5 февраля 2021 г.;

– ГОСТ 15971-90 «Системы обработки информации. Термины и определения», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 октября 1990 г. № 2698;

– ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 августа 1990 г. № 2467;

– ГОСТ 29099-91 «Сети вычислительные локальные. Термины и определения», утвержденный постановлением Комитета стандартизации и метрологии СССР от 25 сентября 1991 г. № 1491;

– ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1520-ст;

– ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1521-ст;

– ГОСТ 34-601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 29 декабря 1990 г. № 3469;

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», утвержденный постановлением Госстандарта России от 9 февраля 1995 г. № 49;

– ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст;

– ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство», утвержденный постановлением Госстандарта России от 14 июля 1998 г. № 295;

– ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст;

– ГОСТ Р 2.105-2019 «Единая система конструкторской документации. Общие требования к текстовым документам», утвержденный приказом Росстандарта от 29 апреля 2019 г. № 175-ст;

– ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов», утвержденный приказом Росстандарта от 25 октября 2021 г. № 1297-ст;

– руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», утвержденный Решением председателя Гостехкомиссии России от 30 марта 1992 г.

Приложение 2

Соответствие возможных целей реализации угроз безопасности информации с негативными последствиями

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Виды риска (ущерба)		
			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**
1.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды;	-	-	НП.1, НП.2
		Любопытство или желание самореализации (подтверждение статуса).	-	-	
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих	Получение финансовой иной материальной выгоды;	-	-	НП.1, НП.2
		Получение конкурентных преимуществ;	-	-	
		Непреднамеренные, неосторожные или неквалифицированные действия.	-	-	
3.	Поставщики вычислительных услуг, услуг связи	Получение финансовой иной материальной выгоды;	-	-	НП.1, НП.2
		Получение конкурентных преимуществ;	-	-	
		Непреднамеренные, неосторожные или неквалифицированные действия.	-	-	
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой иной материальной выгоды;	-	-	НП.1, НП.2
		Получение конкурентных преимуществ;	-	-	
		Непреднамеренные, неосторожные или неквалифицированные действия.	-	-	
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой иной материальной выгоды;	-	-	НП.1, НП.2
		Непреднамеренные, неосторожные или неквалифицированные	-	-	

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Виды риска (ущерба)		
			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
		действия.			
6.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды;	-	-	НП.1, НП.2
		Любопытство или желание самореализации (подтверждение статуса);	-	-	
		Непреднамеренные, неосторожные или неквалифицированные действия;	-	-	
		Месть за ранее совершенные действия.	-	-	
7.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды;	-	-	НП.1, НП.2
		Любопытство или желание самореализации (подтверждение статуса);	-	-	
		Непреднамеренные, неосторожные или неквалифицированные действия;	-	-	
		Месть за ранее совершенные действия.	-	-	

Приложение 3

Уровни возможностей нарушителя

№	Уровень возможностей нарушителей	Возможности нарушителя по реализации угроз безопасности
1	**2**	**3**
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
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
Н3	Нарушитель, обладающий средними возможностями	– обладает всеми возможностями нарушителей с базовыми повышенными возможностями; – имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей); – имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей); – имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. – имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению,

1	2	3
		телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа; – обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. – обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах; – имеет возможность реализовывать угрозы безопасности информации в составе группы лиц
Н4	Нарушитель, обладающий высокими возможностями	– обладает всеми возможностями нарушителей со средними возможностями; – имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня»; – имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств; – имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение; – имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности; – имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. – имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации; – обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей

Приложение 4

Перечень исключенных угроз
из базового перечня угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Обоснование исключение из числа возможных угроз безопасности информации
1	2	3
УБИ.001-003	Угроза автоматического распространения вредоносного кода в грид-системе	Отсутствуют объекты воздействия
	Угроза агрегирования данных, передаваемых в грид-системе	
	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Уровень возможностей нарушителя недостаточен для реализации угрозы
УБИ.010-011	Угроза выхода процесса за пределы виртуальной машины	Отсутствуют объекты воздействия
	Угроза деавторизации санкционированного клиента беспроводной сети	
УБИ.016-017	Угроза доступа к локальным файлам сервера при помощи URL	
	Угроза доступа/перехвата/изменения HTTP cookies	
УБИ.019-021	Угроза заражения DNS-кеша	
	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	
	Угроза злоупотребления доверием потребителей облачных услуг	
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Уровень возможностей нарушителя недостаточен для реализации угрозы
УБИ.026	Угроза искажения XML-схемы	Отсутствуют объекты воздействия
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Уровень возможностей нарушителя недостаточен для реализации угрозы
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Отсутствуют объекты воздействия
УБИ.040-048	Угроза конфликта юрисдикций различных стран	
	Угроза межсайтового скриптинга	
	Угроза межсайтовой подделки запроса	
	Угроза нарушения доступности облачного сервера	
	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	
	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	
	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	
	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	
УБИ.054-062	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	
	Угроза незащищённого администрирования облачных услуг	
	Угроза некачественного переноса инфраструктуры в облако	
	Угроза неконтролируемого копирования данных внутри	

1	2	3
	хранилища больших данных	
	Угроза неконтролируемого роста числа виртуальных машин	
	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	
	Угроза неконтролируемого уничтожения информации хранилищем больших данных	
	Угроза некорректного задания структуры данных транзакции	
	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	
УБИ.064-066	Угроза некорректной реализации политики лицензирования в облаке	
	Угроза неопределённости в распределении ответственности между ролями в облаке	
	Угроза неопределённости ответственности за обеспечение безопасности облака	
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	
УБИ.075-085	Угроза несанкционированного доступа к виртуальным каналам передачи	
	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	
	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	
	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	
	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	
	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	
	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	
	Угроза несанкционированного доступа к сегментам вычислительного поля	
	Угроза несанкционированного доступа к системе по беспроводным каналам	
	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	
	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	
УБИ.089	Угроза несанкционированного редактирования реестра	
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	
УБИ.096-097	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	
	Угроза несогласованности правил доступа к большим данным	
УБИ.101	Угроза общедоступности облачной инфраструктуры	
УБИ.105-108	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	
	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	
	Угроза отключения контрольных датчиков	
	Угроза ошибки обновления гипервизора	
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	

1	2	3
УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	
УБИ.119-121	Угроза перехвата управления гипервизором	
	Угроза перехвата управления средой виртуализации	
	Угроза повреждения системного реестра	
УБИ.125-126	Угроза подключения к беспроводной сети в обход процедуры аутентификации	
	Угроза подмены беспроводного клиента или точки доступа	
УБИ.133-138	Угроза получения сведений о владельце беспроводного устройства	
	Угроза потери доверия к поставщику облачных услуг	
	Угроза потери и утечки данных, обрабатываемых в облаке	
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	
	Угроза потери управления облачными ресурсами	
	Угроза потери управления собственной инфраструктурой при переносе её в облако	
УБИ.139	Угроза преодоления физической защиты	Для реализации данной угрозы отсутствуют актуальные способы реализации. Т.е. возможности актуальных нарушителей не позволяют использовать способы реализации данной угрозы или отсутствуют условия (доступ к объектам воздействия), при которых способы реализации данной угрозы могут быть реализованы в отношении объектов воздействия, на которые направлена данная угроза
УБИ.141-142	Угроза привязки к поставщику облачных услуг	Отсутствуют объекты воздействия
	Угроза приостановки оказания облачных услуг вследствие технических сбоев	
УБИ.146-148	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	
	Угроза распространения несанкционированно повышенных прав на всю грид-систему	
	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	
УБИ.159	Угроза «форсированного веб-браузинга»	
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	
УБИ.172-175	Угроза распространения «почтовых червей»	
	Угроза «спама» веб-сервера	
	Угроза «фарминга»	
	Угроза «фишинга»	
УБИ.180-181	Угроза отказа подсистемы обеспечения температурного режима	
	Угроза перехвата одноразовых паролей в режиме реального времени	
УБИ.183-184	Угроза перехвата управления автоматизированной системой управления технологическими процессами	

1	2	3
	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Для реализации данной угрозы отсутствуют актуальные способы реализации. Т.е. возможности актуальных нарушителей не позволяют использовать способы реализации данной угрозы или отсутствуют условия (доступ к объектам воздействия), при которых способы реализации данной угрозы могут быть реализованы в отношении объектов воздействия, на которые направлена данная угроза
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Отсутствуют объекты воздействия
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Уровень возможностей нарушителя недостаточен для реализации угрозы
УБИ.196-197	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Отсутствуют объекты воздействия
	Угроза хищения аутентификационной информации из временных файлов cookie	
УБИ.199-200	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	
	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Для реализации данной угрозы отсутствуют актуальные способы реализации. Т.е. возможности актуальных нарушителей не позволяют использовать способы реализации данной угрозы или отсутствуют условия (доступ к объектам воздействия), при которых способы реализации данной угрозы могут быть реализованы в отношении объектов воздействия, на которые направлена данная угроза
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Отсутствуют объекты воздействия
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Уровень возможностей нарушителя недостаточен для реализации угрозы

1	2	3
УБИ.213	Угроза обхода многофакторной аутентификации	
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Отсутствуют объекты воздействия
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Для реализации данной угрозы отсутствуют актуальные способы реализации
УБИ.218-222	Угроза раскрытия информации о модели машинного обучения	Отсутствуют объекты воздействия
	Угроза хищения обучающих данных	
	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	
	Угроза автоматического распространения вредоносного кода в грид-системе	
	Угроза агрегирования данных, передаваемых в грид-системе	

Приложение 5

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок
		Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.
		Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.
		Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.
		Т1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
		Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
		Т1.9. 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.
		Т1.10. Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы)
		Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
		Т1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
		Т1.13. Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения
		Т1.14. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации
		Т1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках
		Т1.16. Сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного

№	Тактика	Основные техники
		оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров
		Т1.17. Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		Т1.18. Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		Т1.19. Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		Т1.20. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
Т2	Получение первоначального доступа к компонентам систем и сетей	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
		Т2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра.
		Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.
		Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.
		Т2.6. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок
		Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.
		Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
		Т2.9. Несанкционированное подключение внешних устройств. Пример: несанкционированное подключение точки доступа Wi-Fi
		Т2.10. 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)

№	Тактика	Основные техники
		Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
		Т2.12. Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа.
		Т2.13. Реализация атаки типа «человек посередине» для осуществления доступа, например, NTLM/SMB Relaying атаки
		Т2.14. Доступ путем эксплуатации недостатков систем биометрической аутентификации.
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
		Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей
		Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
		Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами
		Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution)
		Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных
		Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе.
		Т3.8. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.
		Т3.9. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.
		Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
		Т3.11. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «даркверб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т3.12. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.13. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.14. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в

№	Тактика	Основные техники
		том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
		Т3.15. Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии
		Т3.16. Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL.
Т4	Закрепление (сохранение доступа) в системе или сети	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных
		Т4.2. Использование штатных средств удаленного доступа и управления операционной системы
		Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы. Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода
		Т4.4. Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)
		Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети
		Т4.6. Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков
		Т4.7. Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Т5.1. Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования.
		Т5.2. Использование штатных средств удаленного доступа и управления операционной системы
		Т5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		Т5.4. Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		Т5.5. Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т5.6. Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения.
		Т5.7. Туннелирование трафика управления через VPN
		Т5.8. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие

№	Тактика	Основные техники
		Т5.9. Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети
		Т5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления
		Т5.11. Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п.
		Т5.12. Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.
		Т5.13. Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения
Т6	Повышение привилегий по доступу к компонентам систем и сетей	Т6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими
		Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
		Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий.
		Т6.4. Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи).
		Т6.5. Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций.
		Т6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима.
		Т6.7. Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями.
		Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей.
		Т6.9. Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды.
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.
		Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
		Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
		Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов
		Т7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы

№	Тактика	Основные техники
		управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
		Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности
		Т7.7. Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных
		Т7.8. Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов, или о других признаках атаки
		Т7.9. Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей.
		Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения
		Т7.11. Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе.
		Т7.12. Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности.
		Т7.13. Создание скрытых файлов, скрытых учетных записей
		Т7.14. Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов
		Т7.15. Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки
		Т7.16. Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки.
		Т7.17. Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети
		Т7.18. Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе
		Т7.19. Туннелирование трафика управления через VPN
		Т7.20. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т7.21. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков
		Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе.
		Т7.24. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.

№	Тактика	Основные техники
		Т7.25. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.
		Т7.26. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах.
		Т7.27. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т7.28. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т7.29. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Т8.1. Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа
		Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям
		Т8.3. Использование механизмов дистанционной установки программного обеспечения и конфигурирования.
		Т8.4. Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям
		Т8.5. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т8.6. Копирование вредоносного кода на съемные носители
		Т8.7. Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети
		Т8.8. Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях.
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Т9.1. Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования.
		Т9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы
		Т9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		Т9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств

№	Тактика	Основные техники
		Т9.5. Отправка данных по известным протоколам управления и передачи данных
		Т9.6. Отправка данных по собственным протоколам
		Т9.7. Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения.
		Т9.8. Туннелирование трафика передачи данных через VPN
		Т9.9. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т9.10. Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т9.11. Отправка данных через альтернативную среду передачи данных.
		Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации
		Т9.13. Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей
		Т9.14. Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети)
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
		Т10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа
		Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения
		Т10.4. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения
		Т10.5. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения
		Т10.6. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства
		Т10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей
		Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей
		Т10.9. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)
		Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
		Т10.11. Нецелевое использование ресурсов системы.
		Т10.12. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов.
		Т10.13. Несанкционированное воздействие на автоматизированные

№	Тактика	Основные техники
		системы управления с целью вызова отказа или поломки оборудования, в том числе АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.14. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.15. Воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой.

Приложение 6

Результаты оценки возможных угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
1	2	3	4	5	6	7
УБИ.004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.7, СР.9	Т1.9, Т1.15, Т1.16, Т2.9
УБИ.006	Угроза внедрения кода или данных	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.2, СР.6, СР.7	Т1.4, Т1.5, Т2.5, Т2.10, Т3.1, Т3.2, Т3.15, Т4.2, Т5.2
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.8	Т1.9, Т1.16, Т2.6, Т3.5, Т6.2, Т6.3
УБИ.008	Угроза	Внешний	Системное	НП.1,	СР.1,	Т1.6,

1	2	3	4	5	6	7
	восстановления и/или повторного использования аутентификацион-ной информации	нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	ПО, Микропрограммное обеспечение, Учетные данные пользователя	НП.2	СР.7, СР.8	Т2.10, Т4.1
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.7, СР.8	Т1.9, Т3.18, Т4.8
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Объекты файловой системы, Прикладное ПО	НП.1, НП.2	СР.1, СР.8	Т1.9, Т1.16, Т2.5, Т2.6, Т3.7
Идентификатор	Наименование угрозы	Характеристика нарушителя,	Объект воздействия	Негативные	Способы	Возможные

1	2	3	4	5	6	7
угрозы		необходимая для реализации угрозы		послед ствия	реализа ции угрозы	сценари и реализа ции угрозы
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.8	Т1.9, Т1.16, Т2.5, Т4.6
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислитель ной сети (автоматизи рованные рабочие места, серверы, маршрутизат оры, коммутатор ы, IoT-устройства и т.п.) машинный носитель информации в составе СВТ	НП.1, НП.2	СР.1, СР.8	Т1.5, Т1.16, Т1.19, Т2.5, Т2.6
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель,	Объекты файловой системы	НП.1, НП.2	СР.1	Т1.9, Т1.16, Т2.3, Т2.5, Т2.6, Т6.3, Т6.6

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.7	Т2.5, Т10.2
УБИ.022	Угроза избыточного выделения оперативной памяти	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий	Сетевое ПО, Системное ПО	НП.1, НП.2	СР.2, СР.4	Т2.3, Т2.4, Т2.5, Т3.2, Т3.3

1	2	3	4	5	6	7
		базовыми повышенными возможностями				
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, СВТ, Прикладное ПО	НП.1, НП.2	СР.1, СР.4	Т2.7, Т3.7, Т10.3
УБИ.025	Угроза изменения системных и глобальных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1	Т10.2, Т10.4
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.2	Т3.2, Т8.1
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий	Объекты файловой системы	НП.1, НП.2	СР.1, СР.2	Т1.5, Т1.9, Т10.1

1	2	3	4	5	6	7
		базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, СЗИ, Прикладное ПО	НП.1, НП.2	СР.1, СР.7	Т1.1, Т1.9, Т1.16, Т2.4
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.7	Т1.5, Т1.9, Т1.16, Т2.4, Т2.5, Т6.3, Т6.6

1	2	3	4	5	6	7
		повышенными возможностями				
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Внешний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.2, СР.7	Т1.16, Т2.12, Т3.8, Т3.11, Т4.6
УБИ.033	Угроза использования слабостей кодирования входных данных	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	НП.1, НП.2	СР.1, СР.7, СР.8	Т1.5, Т2.5, Т2.6, Т10.2
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Системное ПО	НП.1, НП.2	СР.1	Т1.5, Т1.9, Т2.3, Т2.5, Т10.1
УБИ.036	Угроза исследования механизмов	Внешний нарушитель, обладающий	Сетевое ПО, Системное ПО,	НП.1, НП.2	СР.7	Т2.5

1	2	3	4	5	6	7
	работы программы	базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное ПО			
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	НП.1, НП.2	СР.1, СР.7	Т1.9, Т2.5, Т2.6
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Внешний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1	Т1.5, Т2.5, Т4.6
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1	Т1.5, Т1.9, Т1.16, Т2.5, Т4.6, Т10.2, Т10.6
УБИ.049	Угроза нарушения целостности данных кеша	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель,	Сетевое ПО	НП.1, НП.2	СР.1, СР.8	Т2.5, Т3.9, Т10.1, Т10.2

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1, НП.2	СР.8	Т10.8
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.10	Т2.5
УБИ.063	Угроза некорректного использования функционала программного и	Внешний нарушитель, обладающий базовыми повышенными	Сетевое ПО, Системное ПО, Микропрограммное	НП.1, НП.2	СР.1, СР.8	Т2.5, Т10.11

1	2	3	4	5	6	7
	аппаратного обеспечения	возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	обеспечение, Прикладное ПО			
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	НП.1, НП.2	СР.1, СР.7, СР.8	Т1.13, Т1.14, Т10.1
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	НП.1, НП.2	СР.1, СР.8	Т1.5, Т2.5, Т10.3
УБИ.069	Угроза неправомерных действий в каналах связи	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик	НП.1, НП.2	СР.1, СР.8	Т1.5, Т2.5, Т10.8
УБИ.071	Угроза несанкционированного восстановления	Внешний нарушитель, обладающий базовыми	Машинный носитель информации в составе	НП.1, НП.2	СР.1, СР.7, СР.8	Т1.9, Т2.5, Т10.1

1	2	3	4	5	6	7
	удалённой защищаемой информации	возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СВТ			
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.2, СР.7, СР.8	Т2.5, Т3.8, Т3.18
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Сетевое ПО, Микропрограммное обеспечение	НП.1, НП.2	СР.1, СР.2, СР.8	Т1.5, Т2.5, Т4.6
УБИ.074	Угроза несанкционированного доступа к	Внешний нарушитель, обладающий	Системное ПО, Машинный	НП.1, НП.2	СР.1, СР.7, СР.8	Т1.12, Т2.5, Т10.1

1	2	3	4	5	6	7
	аутентификационной информации	базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	носитель информации в составе СВТ, Учетные данные пользователя, Объекты файловой системы			
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Учетные данные пользователя, Объекты файловой системы	НП.1, НП.2	СР.1, СР.7	Т1.5, Т1.12, Т1.22, Т2.4, Т2.11, Т4.1, Т10.1
УБИ.087	Угроза несанкционированного использования	Внутренний нарушитель, обладающий базовыми	BIOS/UEFI	НП.1, НП.2	СР.1, СР.8	Т1.5, Т1.9, Т1.16, Т2.5

1	2	3	4	5	6	7
	привилегированных функций BIOS	возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе СВТ, Объекты файловой системы	НП.1, НП.2	СР.1	Т2.4, Т2.9, Т10.1
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Системное ПО	НП.1, НП.2	СР.1, СР.7	Т1.5, Т2.4, Т4.1, Т5.2, Т10.2

1	2	3	4	5	6	7
		Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе СВТ, Объекты файловой системы	НП.1, НП.2	СР.1, СР.7	Т1.5, Т2.5, Т10.8
УБИ.093	Угроза несанкционированного управления буфером	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1	Т1.9, Т2.4, Т2.5, Т3.2, Т10.1

1	2	3	4	5	6	7
		нарушитель, обладающий базовыми повышенными возможностями				
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	НП.1, НП.2	СР.1, СР.7	Т1.5, Т2.5, Т10.1, Т10.3
УБИ.095	Угроза несанкционированного управления указателями	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.2	Т1.5, Т2.4, Т2.11, Т3.2, Т10.3, Т10.4
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1, НП.2	СР.1	Т1.4, Т1.5, Т1.22, Т2.3, Т10.1

1	2	3	4	5	6	7
УБИ.099	Угроза обнаружения хостов	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1, НП.2	СР.1, СР.7	Т1.4, Т1.5, Т1.22, Т2.3, Т10.1
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.7, СР.8	Т2.4, Т2.5, Т4.1, Т6.6
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.7, СР.8	Т2.5

1	2	3	4	5	6	7
		нарушитель, обладающий базовыми повышенными возможностями				
УБИ.103	Угроза определения типов объектов защиты	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1, НП.2	СР.7, СР.8	Т1.1, Т1.3, Т2.4
УБИ.104	Угроза определения топологии вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1, НП.2	СР.1	Т1.4, Т1.5, Т1.22, Т2.3
УБИ.109	Угроза перебора всех настроек и параметров приложения	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель,	Сетевое ПО, Системное ПО, Микропрограммное обеспечение	НП.1, НП.2	СР.1, СР.8	Т2.5, Т2.6, Т10.10

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями				
УБИ.111	Угроза передачи данных по скрытым каналам	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик, Системное ПО	НП.1, НП.2	СР.1, СР.7	Т2.4, Т9.10
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СВТ	НП.1, НП.2	СР.1	Т2.5, Т2.11, Т10.8
УБИ.114	Угроза переполнения целочисленных переменных	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1	Т1.1, Т1.5, Т1.9, Т2.5, Т10.1

1	2	3	4	5	6	7
		нарушитель, обладающий базовыми повышенными возможностями				
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.2	Т1.4, Т1.12, Т2.4, Т2.5, Т2.11, Т3.1, Т4.1, Т10.1, Т10.3
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик	НП.1, НП.2	СР.1, СР.8	Т1.3, Т2.4, Т2.5, Т2.11
УБИ.117	Угроза перехвата привилегированного потока	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1	Т1.5, Т2.4, Т2.5, Т2.11, Т6.1

1	2	3	4	5	6	7
		нарушитель, обладающий базовыми повышенными возможностями				
УБИ.118	Угроза перехвата привилегированного процесса	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1	Т1.5, Т2.4, Т2.5, Т2.11, Т3.1, Т4.1, Т6.3
УБИ.122	Угроза повышения привилегий	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО	НП.1, НП.2	СР.1, СР.2, СР.7	Т2.5, Т3.5, Т6.1, Т10.3
УБИ.123	Угроза подбора пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.7	Т1.6, Т2.5, Т2.10, Т4.1, Т10.1
УБИ.124	Угроза подделки записей журнала регистрации событий	Внешний нарушитель, обладающий базовыми возможностями,	Сетевое ПО, Системное ПО, СЗИ, Объекты файловой	НП.1, НП.2	СР.1, СР.7	Т1.22, Т2.5, Т2.11, Т7.6

1	2	3	4	5	6	7
		Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	системы, Прикладное ПО			
УБИ.127	Угроза подмены действия пользователя путём обмана	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.8	Т1.11, Т2.8, Т2.11
УБИ.128	Угроза подмены доверенного пользователя	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1, НП.2	СР.1	Т1.5, Т2.5, Т2.9
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель,	BIOS/UEFI	НП.1, НП.2	СР.1, СР.7	Т1.5, Т2.5, Т3.7, Т4.6, Т4.7

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями				
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Прикладное ПО	НП.1, НП.2	СР.1, СР.7	Т1.5, Т2.5, Т2.11, Т10.2
УБИ.131	Угроза подмены субъекта сетевого доступа	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Прикладное ПО	НП.1, НП.2	СР.1	Т1.2, Т2.5, Т10.1
УБИ.132	Угроза получения предварительной информации об объекте защиты	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, и т.п.), Прикладное ПО	НП.1, НП.2	СР.1, СР.7	Т1.5, Т1.6, Т1.17
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий	Сетевое ПО, Сетевой трафик, Системное ПО, Узел вычислительной сети (автоматизи	НП.1, НП.2	СР.1, СР.8, СР.11	Т2.3, Т2.5, Т2.2

1	2	3	4	5	6	7
		базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	рованные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.) машинный носитель информации в составе СВТ			
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Машинный носитель информации в составе СВТ, Микропрограммное обеспечение	НП.1, НП.2	СР.1, СР.8	Т1.5, Т2.5, Т7.8, Т10.10
УБИ.144	Угроза программного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1	Т1.9, Т1.22, Т2.4, Т2.11, Т10.6
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель,	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.2	Т2.4, Т2.5, Т2.8, Т3.3

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, Объекты файловой системы	НП.1, НП.2	СР.1, СР.4	Т1.5, Т2.5, Т10.10
УБИ.150	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.8	Т1.5, Т2.5, Т4.6
УБИ.152	Угроза удаления аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний	Системное ПО, Микропрограммное обеспечение, Учетные данные пользователя	НП.1, НП.2	СР.1, СР.7	Т1.22, Т2.4, Т2.11, Т10.10

1	2	3	4	5	6	7
		нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)	НП.1, НП.2	СР.1, СР.7	Т1.2, Т1.22, Т2.3, Т2.5
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.1, НП.2	СР.1, СР.8	Т1.5, Т2.5, Т3.8, Т4.6, Т7.22, Т10.6, Т10.10
УБИ.155	Угроза утраты	Внешний	Сетевое ПО,	НП.1,	СР.1,	Т1.5,

1	2	3	4	5	6	7
	вычислительных ресурсов	нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик, Системное ПО, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.) машинный носитель информации в составе СВТ	НП.2	СР.7	Т1.9, Т2.3, Т2.5, Т2.11, Т10.10
УБИ.156	Угроза утраты носителей информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе СВТ	НП.1, НП.2	СР.1, СР.7, СР.8	Т1.10, Т10.1, Т10.8
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ	НП.1, НП.2	СР.1, СР.8, СР.10	Т2.2, Т10.8, Т10.10
УБИ.158	Угроза	Внешний	Машинный	НП.1,	СР.1,	Т2.2,

1	2	3	4	5	6	7
	форматирования носителей информации	нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	носитель информации в составе СВТ	НП.2	СР.8	Т2.5, Т10.8
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ, машинный носитель информации в составе СВТ	НП.1, НП.2	СР.1, СР.8	Т2.5
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель,	Сетевое ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.4	Т1.10, Т3.11, Т3.16

1	2	3	4	5	6	7
		обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	НП.1, НП.2	СР.1, СР.8	Т1.3, Т2.5, Т10.1
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1, НП.2	СР.8	Т2.5
УБИ.166	Угроза внедрения системной избыточности	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1, НП.2	СР.8	Т2.5
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Учетные данные пользователя	НП.1, НП.2	СР.1	Т1.3, Т1.6, Т1.9, Т1.11, Т1.15, Т2.8, Т2.11, Т4.1
УБИ.169	Угроза наличия	Внутренний	Сетевое ПО,	НП.1,	СР.1,	Т2.5,

1	2	3	4	5	6	7
	механизмов разработчика	нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, Прикладное ПО	НП.2	СР.8	Т2.6, Т3.12
УБИ.170	Угроза неправомерного шифрования информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.1, НП.2	СР.4	Т2.4, Т3.3, Т10.8
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)	НП.1, НП.2	СР.2, СР.7	Т1.2, Т2.3, Т2.4, Т2.5, Т3.1, Т4.3
УБИ.176	Угроза нарушения технологического/ производственного процесса из-за временны́х задержек, вносимых средством защиты	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	СЗИ	НП.1, НП.2	СР.1, СР.7, СР.11	Т1.4, Т1.5, Т2.3, Т2.5, Т10.3, Т10.10
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.8	Т10.14

1	2	3	4	5	6	7
	безопасностью	нарушитель, обладающий базовыми повышенными возможностями				
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	НП.1, НП.2	СР.1	Т2.4, Т2.5, Т10.5
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель,	Объекты файловой системы	НП.1, НП.2	СР.7, СР.10	Т2.5, Т10.7, Т10.8

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями				
УБИ.182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ	НП.1, НП.2	СР.1, СР.8	Т10.8, Т10.10
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СЗИ	НП.1, НП.2	СР.1, СР.8	Т2.4, Т7.4
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель,	СЗИ	НП.1, НП.2	СР.1, СР.7, СР.8	Т2.4, Т7.4, Т10.2

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями				
УБИ.188	Угроза подмены программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.2, СР.8	Т2.7, Т3.7, Т3.8, Т3.10, Т7.24, Т10.7
УБИ.189	Угроза маскирования действий вредоносного кода	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО	НП.1, НП.2	СР.1, СР.2, СР.7	Т2.4, Т3.7, Т7.1
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.2, СР.7, СР.8	Т2.7, Т3.2
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель,	Сетевое ПО, Системное ПО, Прикладное ПО	НП.1, НП.2	СР.1, СР.8	Т2.5, Т10.2

1	2	3	4	5	6	7
		обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Внешний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	НП.1, НП.2	СР.2, СР.7	Т1.5, Т1.6, Т1.12, Т2.6, Т4.1, Т7.12, Т7.13
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ	НП.1, НП.2	СР.1, СР.2, СР.7	Т2.5, Т3.2, Т6.3, Т9.11
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	СВТ	НП.1, НП.2	СР.1, СР.7	Т2.4

1	2	3	4	5	6	7
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СВТ	НП.1, НП.2	СР.2, СР.7	Т1.5, Т1.11, Т2.7, Т10.11
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СВТ	НП.1, НП.2	СР.1	Т1.5, Т1.9, Т2.4, Т10.1, Т10.5
УБИ.211	Угроза	Внутренний	Системное	НП.1,	СР.1,	Т10.2

1	2	3	4	5	6	7
	использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	ПО	НП.2	СР.8	
УБИ.212	Угроза перехвата управления информационной системой	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, СВТ, Информационная (автоматизированная) система	НП.1, НП.2	СР.1	Т2.4, Т2.5, Т8.1, Т10.1
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1, НП.2	СР.1, СР.7	Т7.4
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Внешний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1, НП.2	СР.1, СР.8	Т1.5, Т7.25, Т10.2

Приложение 7

Анализ достаточность принятых мер для нейтрализации угроз безопасности информации с учетом принятой модели нарушителя и способов реализации угроз

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Способы реализации угрозы	Подсистема системы защиты информации от НСД
1	2	3	4	5	6
УБИ.004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.7, СР.9	Организационно-техническая подсистема Подсистема защиты от несанкционированной начальной загрузки
УБИ.006	Угроза внедрения кода или данных	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.2, СР.6, СР.7	Подсистема обеспечения целостности Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Криптографическая подсистема в каналах связи Подсистема резервного копирования и восстановления данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.8	Подсистема обеспечения целостности Подсистема межсетевого экранирования Подсистема обнаружения и

1	2	3	4	5	6
		возможностями			предотвращения вторжения Криптографическая подсистема в каналах связи Подсистема резервного копирования и восстановления данных
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, Микропрограммное обеспечение, Учетные данные пользователя	СР.1, СР.7, СР.8	Подсистема управления доступом Подсистема регистрации и учета Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.7, СР.8	Организационно-техническая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема защиты от несанкционированной начальной загрузки
УБИ.012	Угроза деструктивного изменения конфигура	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний	Сетевое ПО, Системное ПО, Микропрограммное	СР.1, СР.8	Подсистема антивирусной защиты Подсистема управления

1	2	3	4	5	6
	ции/среды окружения программ	нарушитель, обладающий базовыми повышенными возможностями	обеспечение, Объекты файловой системы, Прикладное ПО		доступом Подсистема обеспечения целостности Подсистема регистрации и учета
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.8	Организационно-техническая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема защиты от несанкционированной начальной загрузки
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.) машинный носитель информации в составе СВТ	СР.1, СР.8	Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Криптографическая подсистема в каналах связи
УБИ.015	Угроза доступа к	Внешний нарушитель, обладающий базовыми	Объекты файловой	СР.1	Подсистема управления

1	2	3	4	5	6
	защищаемым файлам с использованием обходного пути	возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	системы		доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема обеспечения целостности Подсистема антивирусной защиты Организационно-техническая подсистема
УБИ.018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.7	Организационно-техническая подсистема Подсистема защиты от несанкционированной начальной загрузки
УБИ.022	Угроза избыточного выделения оперативной памяти	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО	СР.2, СР.4	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования
УБИ.023	Угроза изменения компонент	Внутренний нарушитель, обладающий базовыми	Системное ПО, СВТ, Прикладное	СР.1, СР.4	Подсистема антивирусной защиты

1	2	3	4	5	6
	ов информационной (автоматизированной) системы	возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	ПО		Подсистема обеспечения целостности Подсистема защиты от несанкционированной начальной загрузки Подсистема управления доступом Подсистема регистрации и учета Организационно-техническая подсистема
УБИ.025	Угроза изменения системных и глобальных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1	Подсистема управления доступом Подсистема обеспечения целостности Организационно-техническая подсистема Подсистема защиты от несанкционированной начальной загрузки
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.2	Подсистема антивирусной защиты Подсистема управления доступом Подсистема обеспечения целостности
УБИ.028	Угроза использования	Внешний нарушитель, обладающий базовыми возможностями,	Объекты файловой системы	СР.1, СР.2	Подсистема обнаружения и предотвращения

1	2	3	4	5	6
	альтернативных путей доступа к ресурсам	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями			вторжения Подсистема межсетевого экранирования Подсистема управления доступом Подсистема регистрации и учета
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, СЗИ, Прикладное ПО	СР.1, СР.7	Подсистема управления доступом Подсистема защиты от несанкционированной начальной загрузки Подсистема регистрации и учета Подсистема межсетевого экранирования Подсистема управления комплексом средств защиты
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми	Сетевое ПО, Системное ПО, Прикладное ПО	СР.7	Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом

1	2	3	4	5	6
		повышенными возможностями			
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Внешний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.2, СР.7	Подсистема защиты от несанкционированной начальной загрузки Подсистема обеспечения целостности Организационно-техническая подсистема
УБИ.033	Угроза использования слабостей кодирования входных данных	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	СР.1, СР.7, СР.8	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом Подсистема регистрации и учета
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Системное ПО	СР.1	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом Подсистема регистрации и учета

1	2	3	4	5	6
УБИ.036	Угроза исследования механизмов работы программы	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	СР.7	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	СР.1, СР.7	Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Внешний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1	Подсистема защиты от несанкционированной начальной загрузки Подсистема обеспечения целостности Организационно-техническая

1	2	3	4	5	6
					подсистема
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1	Подсистема защиты от несанкционированной начальной загрузки Подсистема обеспечения целостности Организационно-техническая подсистема
УБИ.049	Угроза нарушения целостности данных кеша	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО	СР.1, СР.8	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема обеспечения целостности
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)	СР.8	Подсистема управления доступом Организационно-техническая подсистема Подсистема резервного копирования и восстановления данных
УБИ.053	Угроза невозможности управлени	Внутренний нарушитель, обладающий базовыми возможностями,	BIOS/UEFI	СР.10	Организационно-техническая подсистема Подсистема

1	2	3	4	5	6
	я правами пользователей BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями			обеспечения целостности Подсистема защиты от несанкционированной начальной загрузки
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	СР.1, СР.8	Организационно-техническая подсистема Подсистема управления доступом
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	СР.1, СР.7, СР.8	Организационно-техническая подсистема Подсистема управления доступом
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение, Прикладное ПО	СР.1, СР.8	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения
УБИ.069	Угроза неправомерных действий в	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель,	Сетевой трафик	СР.1, СР.8	Подсистема обнаружения и предотвращения вторжения

1	2	3	4	5	6
	каналах связи	обладающий базовыми повышенными возможностями			Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе СВТ	СР.1, СР.7, СР.8	Подсистема межсетевого экранирования Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема обеспечения целостности Организационно-техническая подсистема
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.2, СР.7, СР.8	Подсистема защиты от несанкционированной начальной загрузки
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или)	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Сетевое ПО, Микропрограммное обеспечение	СР.1, СР.2, СР.8	Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом

1	2	3	4	5	6
	физическому сетевому оборудованию из физической и (или) виртуальной сети				
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, Машинный носитель информации в составе СВТ, Учетные данные пользователя, Объекты файловой системы	СР.1, СР.7, СР.8	Подсистема управления доступом Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Учетные данные пользователя, Объекты файловой системы	СР.1, СР.7	Подсистема управления доступом Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема регистрации и учета Подсистема обеспечения целостности
УБИ.087	Угроза несанкционированного	Внутренний нарушитель, обладающий базовыми возможностями,	BIOS/UEFI	СР.1, СР.8	Подсистема защиты от несанкционированной начальной

1	2	3	4	5	6
	использования привилегированных функций BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями			загрузки
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе СВТ, Объекты файловой системы	СР.1	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Криптографическая подсистема в каналах связи Подсистема регистрации и учета Подсистема защиты от несанкционированной начальной загрузки
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	СР.1, СР.7	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Криптографическая подсистема в каналах связи Подсистема защиты от несанкционированной начальной загрузки

1	2	3	4	5	6
					Подсистема регистрации и учета
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе СВТ, Объекты файловой системы	СР.1, СР.7	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема защиты от несанкционированной начальной загрузки Подсистема регистрации и учета Подсистема резервного копирования и восстановления данных
УБИ.093	Угроза несанкционированного управления буфером	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема регистрации и учета
УБИ.094	Угроза несанкционированно	Внешний нарушитель, обладающий базовыми повышенными	Сетевое ПО, Системное ПО,	СР.1, СР.7	Подсистема управления доступом

1	2	3	4	5	6
	го управления синхронизацией и состоянием	возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное ПО		Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема регистрации и учета
УБИ.095	Угроза несанкционированного управления указателями	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.2	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема регистрации и учета
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)	СР.1	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.099	Угроза обнаружения хостов	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизи	СР.1, СР.7	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема

1	2	3	4	5	6
			рованные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)		обнаружения и предотвращения вторжения
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.7, СР.8	Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом Подсистема регистрации и учета
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.7, СР.8	Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом Подсистема регистрации и учета
УБИ.103	Угроза определения типов объектов защиты	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные	СР.7, СР.8	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и

1	2	3	4	5	6
			рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)		предотвращения вторжения Подсистема управления доступом Подсистема регистрации и учета
УБИ.104	Угроза определения топологии вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)	СР.1	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.109	Угроза перебора всех настроек и параметров приложения	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Микропрограммное обеспечение	СР.1, СР.8	Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом Подсистема регистрации и учета
УБИ.111	Угроза передачи данных по скрытым каналам	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний	Сетевой трафик, Системное ПО	СР.1, СР.7	Подсистема межсетевого экранирования Подсистема обнаружения и

1	2	3	4	5	6
		нарушитель, обладающий базовыми повышенными возможностями			предотвращения вторжения Подсистема регистрации и учета Подсистема управления доступом
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СВТ	СР.1	Организационно-техническая подсистема Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.114	Угроза переполнения целочисленных переменных	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1	Подсистема управления доступом Подсистема регистрации и учета Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний	Системное ПО, Прикладное ПО	СР.1, СР.2	Подсистема управления доступом Подсистема регистрации и учета

1	2	3	4	5	6
	устройства информации	нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями			
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик	СР.1, СР.8	Подсистема управления доступом Подсистема регистрации и учета Криптографическая подсистема в каналах связи
УБИ.117	Угроза перехвата привилегированного потока	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1	Подсистема управления доступом Подсистема регистрации и учета Организационно-техническая подсистема
УБИ.118	Угроза перехвата привилегированного процесса	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1	Подсистема управления доступом Подсистема регистрации и учета Организационно-техническая подсистема
УБИ.122	Угроза повышения привилегий	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО	СР.1, СР.2, СР.7	Подсистема управления доступом Подсистема регистрации и учета Подсистема защиты от несанкционированной начальной

1	2	3	4	5	6
					загрузки Организационно-техническая подсистема
УБИ.123	Угроза подбора пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.7	Подсистема защиты от несанкционированной начальной загрузки Организационно-техническая подсистема
УБИ.124	Угроза подделки записей журнала регистрации событий	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, СЗИ, Объекты файловой системы, Прикладное ПО	СР.1, СР.7	Подсистема защиты от несанкционированной начальной загрузки Подсистема управления доступом Подсистема регистрации и учета Подсистема резервного копирования и восстановления данных Подсистема межсетевого экранирования
УБИ.127	Угроза подмены действия пользователя путём обмана	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Прикладное ПО	СР.1, СР.8	Организационно-техническая подсистема Подсистема управления доступом Подсистема обеспечения целостности
УБИ.128	Угроза подмены доверенного	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель,	Сетевое ПО, Узел вычислительной сети	СР.1	Организационно-техническая подсистема Подсистема

1	2	3	4	5	6
	пользователя	обладающий базовыми повышенными возможностями	(автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)		управления доступом Подсистема обеспечения целостности
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.7	Организационно-техническая подсистема Подсистема управления доступом Подсистема обеспечения целостности
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Прикладное ПО	СР.1, СР.7	Организационно-техническая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.131	Угроза подмены субъекта сетевого доступа	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Прикладное ПО	СР.1	Организационно-техническая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема межсетевого

1	2	3	4	5	6
					экранирования Подсистема обнаружения и предотвращения вторжения
УБИ.132	Угроза получения предварительной информации об объекте защиты	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы, IoT-устройства и т.п.), Прикладное ПО	СР.1, СР.7	Организационно-техническая подсистема Подсистема управления доступом Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Криптографическая подсистема в каналах связи
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Сетевой трафик, Системное ПО, Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.) машинный носитель информации в составе СВТ	СР.1, СР.8, СР.11	Подсистема управления доступом Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема резервного копирования и восстановления данных

1	2	3	4	5	6
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Машинный носитель информации в составе СВТ, Микропрограммное обеспечение	СР.1, СР.8	Подсистема управления доступом Подсистема обеспечения целостности Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема резервного копирования и восстановления данных
УБИ.144	Угроза программного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1	Подсистема защиты от несанкционированной начальной загрузки Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель,	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.2	Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета Подсистема защиты от несанкционированной начальной

1	2	3	4	5	6
		обладающий базовыми повышенными возможностями			загрузки
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, Объекты файловой системы	СР.1, СР.4	Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета Подсистема резервного копирования и восстановления данных
УБИ.150	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.8	Подсистема защиты от несанкционированной начальной загрузки Подсистема резервного копирования и восстановления данных
УБИ.152	Угроза удаления аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, Микропрограммное обеспечение, Учетные данные пользователя	СР.1, СР.7	Подсистема защиты от несанкционированной начальной загрузки Подсистема резервного копирования и восстановления данных Подсистема управления доступом Подсистема регистрации и учета Подсистема обеспечения

1	2	3	4	5	6
					целостности
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)	СР.1, СР.7	Подсистема обнаружения и предотвращения вторжения Криптографическая подсистема в каналах связи Подсистема межсетевого экранирования
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	СР.1, СР.8	Подсистема защиты от несанкционированной начальной загрузки Подсистема обеспечения целостности Организационно-техническая подсистема Подсистема резервного копирования и восстановления данных
УБИ.155	Угроза утраты вычислительных ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний	Сетевое ПО, Сетевой трафик, Системное ПО, Узел вычислительной сети (автоматизированные рабочие места, серверы,	СР.1, СР.7	Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом Подсистема межсетевого экранирования

1	2	3	4	5	6
		нарушитель, обладающий базовыми повышенными возможностями	маршрутизаторы, коммутаторы и т.п.) машинный носитель информации в составе СВТ		
УБИ.156	Угроза утраты носителей информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе СВТ	СР.1, СР.7, СР.8	Организационно-техническая подсистема Подсистема резервного копирования и восстановления данных
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ	СР.1, СР.8, СР.10	Подсистема резервного копирования и восстановления данных Организационно-техническая подсистема
УБИ.158	Угроза форматирования носителей информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель,	Машинный носитель информации в составе СВТ	СР.1, СР.8	Подсистема защиты от несанкционированной начальной загрузки Подсистема управления доступом Подсистема регистрации и учета Организационно-техническая

1	2	3	4	5	6
		обладающий базовыми повышенными возможностями			подсистема
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ, машинный носитель информации в составе СВТ	СР.1, СР.8	Организационно-техническая подсистема Подсистема регистрации и учета
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Прикладное ПО	СР.1, СР.4	Организационно-техническая подсистема Подсистема регистрации и учета
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	СР.1, СР.8	Подсистема регистрации и учета Подсистема обеспечения целостности Организационно-техническая подсистема Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого

1	2	3	4	5	6
					экранирования
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	СР.8	Организационно-техническая подсистема Подсистема управления доступом Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Криптографическая подсистема в каналах связи Подсистема обеспечения целостности
УБИ.166	Угроза внедрения системной избыточности	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	СР.8	Организационно-техническая подсистема Подсистема управления доступом Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Криптографическая подсистема в каналах связи Подсистема обеспечения целостности
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными	Сетевое ПО, Учетные данные пользователя	СР.1	Организационно-техническая подсистема Подсистема управления доступом

1	2	3	4	5	6
	сервисам	возможностями			Подсистема межсетевого экранирования Подсистема обнаружения и предотвращения вторжения Криптографическая подсистема в каналах связи Подсистема обеспечения целостности Подсистема управления комплексом средств защиты
УБИ.169	Угроза наличия механизмов разработчика	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.8	Организационно-техническая подсистема Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета

1	2	3	4	5	6
УБИ.170	Угроза неправомерного шифрования информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	СР.4	Организационно-техническая подсистема Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета Подсистема межсетевого экранирования Подсистема антивирусной защиты
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, серверы, маршрутизаторы, коммутаторы и т.п.)	СР.2, СР.7	Организационно-техническая подсистема Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета Подсистема межсетевого экранирования Подсистема антивирусной защиты Подсистема обнаружения и предотвращения вторжения Криптографическая подсистема в каналах связи
УБИ.176	Угроза нарушения	Внешний нарушитель, обладающий базовыми	СЗИ	СР.1, СР.7,	Организационно-техническая

1	2	3	4	5	6
	технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями		СР.11	подсистема
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.8	Подсистема управления доступом Подсистема регистрации и учета Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема регистрации и учета
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	СР.1	Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета
УБИ.179	Угроза несанкцио	Внешний нарушитель, обладающий базовыми	Объекты файловой	СР.7, СР.10	Подсистема обеспечения

1	2	3	4	5	6
	нированной модификации защищаемой информации	возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	системы		целостности Подсистема управления доступом Подсистема регистрации и учета Подсистема резервного копирования и восстановления данных Организационно-техническая подсистема Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования
УБИ.182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ	СР.1, СР.8	Организационно-техническая подсистема
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми	СЗИ	СР.1, СР.8	Организационно-техническая подсистема Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета Подсистема резервного

1	2	3	4	5	6
		повышенными возможностями			копирования и восстановления данных Организационно-техническая подсистема Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СЗИ	СР.1, СР.7, СР.8	Организационно-техническая рования
УБИ.188	Угроза подмены программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.2, СР.8	Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета Организационно-техническая подсистема
УБИ.189	Угроза маскирования действий вредоносного кода	Внешний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО	СР.1, СР.2, СР.7	Подсистема антивирусной защиты Подсистема обеспечения целостности Подсистема управления доступом Подсистема

1	2	3	4	5	6
					регистрации и учета Подсистема обнаружения и предотвращения вторжения Организационно-техническая подсистема
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.2, СР.7, СР.8	Подсистема антивирусной защиты Организационно-техническая подсистема Подсистема резервного копирования и восстановления данных Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое ПО, Системное ПО, Прикладное ПО	СР.1, СР.8	Подсистема обеспечения целостности Подсистема управления доступом Подсистема регистрации и учета Организационно-техническая подсистема Подсистема антивирусной защиты

1	2	3	4	5	6
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Внешний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	СР.2, СР.7	Подсистема антивирусной защиты Подсистема управления доступом Подсистема регистрации и учета Подсистема обнаружения и предотвращения вторжения
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, СВТ	СР.1, СР.2, СР.7	Организационно-техническая подсистема Криптографическая подсистема в каналах связи Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями	СВТ	СР.1, СР.7	Подсистема резервного копирования и восстановления данных Организационно-техническая подсистема Подсистема управления комплексом средств защиты
УБИ.208	Угроза	Внешний нарушитель,	СВТ	СР.2,	Организационно-

1	2	3	4	5	6
	нецелевого использования вычислительных ресурсов средства вычислительной техники	обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями		СР.7	техническая подсистема Подсистема обнаружения и предотвращения вторжения Подсистема межсетевого экранирования Подсистема управления доступом Подсистема регистрации и учета Подсистема защиты от несанкционированной начальной загрузки
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Внешний нарушитель, обладающий базовыми возможностями, Внешний нарушитель, обладающий базовыми повышенными возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	СВТ	СР.1	Подсистема управления доступом Подсистема регистрации и учета
УБИ.211	Угроза использования непроверенных пользовательских данных при	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО	СР.1, СР.8	Подсистема резервного копирования и восстановления данных Подсистема управления доступом Подсистема

1	2	3	4	5	6
	формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем				регистрации и учета Подсистема обеспечения целостности
УБИ.212	Угроза перехвата управления информационной системой	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное ПО, СВТ, Информационная (автоматизированная) система	СР.1	Организационно-техническая подсистема Подсистема обнаружения и предотвращения вторжения Подсистема управления доступом Подсистема регистрации и учета Подсистема межсетевого экранирования
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	СР.1, СР.7	Организационно-техническая подсистемаПодсистема регистрации и учета Подсистема управления комплексом средств защиты Подсистема обнаружения и предотвращения

1	2	3	4	5	6
	) системы (в том числе средствам и защиты информации) на события безопасности информации				вторжения Подсистема антивирусной защиты
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Внешний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	СР.1, СР.8	Подсистема межсетевого экранирования Криптографическая подсистема в каналах связи Подсистема обнаружения и предотвращения вторжения Подсистема антивирусной защиты