|  |  |  |  |
| --- | --- | --- | --- |
| **ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ КУРСКОЙ ОБЛАСТИ «ИНФОРМАЦИОННЫЙ ЦЕНТР «РЕГИОН**‑**КУРСК»** | | | |
|  | |  | |
| УТВЕРЖДАЮ | |
| Директор ГУПКО «ИЦ «Регион-Курск» | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_ | И.В. Брагин |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2023 г. | |
| **МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**  **государственная информационная система в сфере финансов Министерства цифрового развития и связи Курской области** | | | |
|  | |  | |
|
|  |  |  |  |
| г. Курск  2023 | | | |

**Оглавление**

[1. Термины и определения 3](#_Toc256000000)

[2. Общие положения 7](#_Toc256000001)

[3. Описание систем и сетей и их характеристика как объектов защиты 10](#_Toc256000002)

[4. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации 15](#_Toc256000003)

[5. Возможные объекты воздействия угроз безопасности информации 17](#_Toc256000004)

[6. Источники угроз безопасности информации 27](#_Toc256000005)

[7. Способы реализации (возникновения) угроз безопасности информации 32](#_Toc256000006)

[8. Актуальные угрозы безопасности информации 50](#_Toc256000007)

[9. Оценка угроз в соответствии с методическими документами ФСБ России 54](#_Toc256000008)

[Приложение № 1 55](#_Toc256000009)

[Приложение № 2 58](#_Toc256000010)

[Приложение № 3 61](#_Toc256000011)

[Приложение № 4 63](#_Toc256000012)

[Приложение № 5 68](#_Toc256000013)

[Приложение № 6 77](#_Toc256000014)

[Приложение № 7 113](#_Toc256000015)

1. 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 ГИС в сфере финансов, 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 ГИС в сфере финансов и не включена оператором системы или сети в границу 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** – 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, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.).

**Информационная система (ИС)** – 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 ГИС в сфере финансов.

**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), 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).

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**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, СКЗИ)** – 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 информативного 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) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

1. Общие положения
   1. **Введение**
      1. Настоящая модель угроз безопасности информации (далее – Модель угроз) содержит результаты оценки угроз безопасности информации.
      2. Оценка угроз проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в государственной информационной системе в сфере финансов Министерства цифрового развития и связи Курской области (далее – ГИС в сфере финансов) (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой в ГИС в сфере финансов информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования ГИС в сфере финансов − актуальных угроз безопасности информации.
   2. **Источники разработки**
      1. 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 определения ГУПКО «ИЦ «Регион‑Курск» (далее – Предприятие) необходимости обеспечения безопасности информации с использованием СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России и ФСБ России.
  + 1. Перечень нормативных правовых актов, методических документов и национальных стандартов, используемый для оценки угроз безопасности информации и разработки Модели угроз, представлен в Приложении № 1.
  1. **Оцениваемые угрозы**
     1. Модель угроз содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей, и техногенных источников угроз. При этом в настоящей Модели угроз не рассматриваются угрозы, связанные с техническими каналами утечки информации (далее – ТКУИ), по причинам, перечисленным в таблице 1.

Таблица 1 – Обоснования исключения угроз, реализуемых за счет ТКУИ

| №  п/п | Угрозы, связан­ные с тех­ни­чес­ки­ми ка­на­ла­ми утеч­ки инфор­ма­ции | Обоснование исключения |
| --- | --- | --- |
| 1. | Угрозы утечки акустической (речевой) информации\* | Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящую специализированную аппаратуру, регистрирующую акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки информации, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.  Характер и объем обрабатываемой в системе информации недоста­то­чен для мотивации нарушителей к реализации таких угроз |
| 2. | Угрозы утечки видовой информации\* | Характеризуются наличием высококвалифицированных нарушителей, использующих специализированные оптические (оптико-электронные) средства для просмотра информации с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав системы.  Характер и объем обрабатываемой в системе информации недостато­чен для мотивации нарушителей к реализации таких угроз |
| 3. | Угрозы утечки информации по каналам ПЭМИН | Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящие специализированные технические средства перехвата побочных (не связанных с прямым функциональным значением элементов системы) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации техническими средствами системы.  Характер и объем обрабатываемой в системе информации недостато­чен для мотивации нарушителей к реализации таких угроз |

\* За исключением угроз, характеризующихся использованием нарушителями портативных (мобильных) устройств съема информации (планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

* 1. **Ответственность за обеспечение защиты информации (безопасности)**
     1. Ответственными за обеспечение безопасности ГИС в сфере финансов приказом Директора ГУПКО «ИЦ «Регион-Курск» назначены должностные лица / подразделения, представленные в таблице 2.

Таблица 2 – Ответственные за обеспечение защиты информации (безопасности)

| №  п/п | Роль под­разде­ле­ния / должностного лица | Должностное лицо / подразделение |
| --- | --- | --- |
| 1. | От­ветс­твен­ный за за­щиту ин­форма­ции, не со­дер­жа­щей све­дения сос­тавля­ющие го­сударс­твен­ную тай­ну | спе­ци­алист по за­щите ин­форма­ции |
| 2. | От­ветс­твен­ный за обес­пе­чение бе­зопас­ности пер­со­наль­ных дан­ных | глав­ный ин­же­нер |
| 3. | От­ветс­твен­ный за пла­ниро­вание и кон­троль ме­роп­ри­ятий по обес­пе­чению ин­форма­ци­он­ной бе­зопас­ности | спе­ци­алист по за­щите ин­форма­ции |
| 4. | От­ветс­твен­ный за уп­равле­ние (ад­ми­нис­три­рова­ние) сис­те­мой за­щиты ин­форма­ции (под­систе­мой бе­зопас­ности) | спе­ци­алист по за­щите ин­форма­ции |
| 5. | От­ветс­твен­ный за вы­яв­ле­ние компь­ютер­ных ин­ци­ден­тов и ре­аги­рова­ние на них | ди­рек­тор;  глав­ный ин­же­нер;  спе­ци­алист по за­щите ин­форма­ции |
| 6. | Сот­рудник, ко­торо­му раз­ре­шены дей­ствия по вне­сению из­ме­нений в кон­фи­гура­цию | глав­ный ин­же­нер |

* 1. **Особенности пересмотра Модели угроз**
     1. Настоящая Модель угроз может быть пересмотрена:
* по решению Предприятия на основе периодически проводимых анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений ГИС в сфере финансов;
* 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 ГИС в сфере финансов;
* в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;
* в случаях выявления инцидентов информационной безопасности в ГИС в сфере финансов и (или) взаимодействующих (смежных) системах.

1. Описание систем и сетей и их характеристика как объектов защиты
   1. **Общее описание объекта оценки угроз**
      1. Настоящая Модель угроз разработана в отношении ГИС в сфере финансов.
      2. Основные характеристики ГИС в сфере финансов:
         1. Основания создания (функционирования):

* Пос­та­нов­ле­ние Гу­бер­на­тора Кур­ской об­ласти от 05.08.2022 г. №229-пг «О соз­да­нии го­сударс­твен­ной ин­форма­ци­он­ной сис­те­мы в сфе­ре фи­нан­сов»,
* Пос­та­нов­ле­ние Гу­бер­на­тора Кур­ской об­ласти от 01.12.2022 г. №388-пг «О по­ряд­ке ве­дения го­сударс­твен­ной ин­форма­ци­он­ной сис­те­мы в сфе­ре фи­нан­сов».
  + - 1. Назначение:  по­выше­ние дос­тупнос­ти ин­форма­ции о фи­нан­со­вой де­ятель­нос­ти ис­полни­тель­ных ор­га­нов Кур­ской об­ласти, го­сударс­твен­ных уч­режде­ний (ор­га­низа­ций) Кур­ской об­ласти;  соз­да­ние инс­тру­мен­тов для вза­имос­вя­зи стра­теги­чес­ко­го и бюд­жетно­го пла­ниро­вания, про­веде­ния мо­нито­рин­га дос­ти­жения фи­нан­со­вых ре­зуль­та­тов ре­али­зации го­сударс­твен­ных прог­рамм Кур­ской об­ласти, а так­же ре­зуль­та­тов, ха­рак­те­ризу­ющих объ­емы и ка­чес­тво ока­зания го­сударс­твен­ных ус­луг и ис­полне­ния го­сударс­твен­ных фун­кций;  обес­пе­чение ин­тегра­ции про­цес­сов сос­тавле­ния и ис­полне­ния об­лас­тно­го бюд­же­та;  обес­пе­чение юри­дичес­ки зна­чимо­го до­кумен­то­обо­рота в со­от­ветс­тву­ющих ин­форма­ци­он­ных сис­те­мах (под­систе­мах) сис­те­мы, ре­али­зу­ющих ее от­дель­ные за­дачи;  ре­шение иных за­дач, пре­дус­мотрен­ных за­коно­датель­ством.
      2. Состав обрабатываемой информации:
* Персональные данные;
* Ключевая, аутентифицирующая и парольная информация;
* Защищаемая информация, относящаяся к системе и ее криптографической защите;
* Информация, содержащаяся в ГИС (о доходах региона и региональных учреждений, ведущих учет платы за оказываемые государственные (муниципальные) услуги);
* Информация, содержащаяся в ГИС (предназначенная для организации централизованного и унифицированного событийно-ориентированного обмена сообщениями между различными информационными системами, используемыми в бюджетном процессе субъектов Российской Федерации и муниципальных образований);
* Информация, содержащаяся в ГИС (предназначенная для составления и ведения сводной бюджетной росписи областного бюджета);
* Информация, содержащаяся в ГИС (предназначенная для составления, анализа и исполнения бюджета субъекта и бюджетов муниципальных образований);
* Информация, содержащаяся в ГИС (предназначенная для формирования консолидированной отчетности всеми участниками бюджетного процесса);
* Информация, содержащаяся в ГИС (предназначенная для формирования реестра расходных обязательств);
* Информация, содержащаяся в ГИС (предназначенная для планирования расходов, прогнозирования доходов, регулирования межбюджетных отношений, формирования, ведения и оценки эффективности государственных (муниципальных) программ, государственных (муниципальных) заданий и планов финансово-хозяйственной деятельности);
* Информация, содержащаяся в ГИС (предназначенная для обеспечения эффективного контроля расходования бюджетных средств на всех этапах планирования, размещения государственного (муниципального) заказа, исполнения контрактов посредством интеграции с Единой информационной системой в сфере закупок в сети Интернет (ЕИС);
* Информация, содержащаяся в ГИС (предназначенная для формирования сводных прогнозов объемов продукции, закупаемой для государственных и муниципальных нужд);
* Информация, содержащаяся в ГИС (сведения о плательщиках - юридических лицах и уплаченных ими налоговых и неналоговых доходах);
* Информация, содержащаяся в ГИС (предназначенная для ведения аналитического бухгалтерского учета исполнения сметы расходов);
* Информация, содержащаяся в ГИС (предназначенная для прогнозирования доходов, формирования реестра расходных обязательств, формирование расчета расходной части бюджета, формирования планов финансово-хозяйственной деятельности);
* Информация, содержащаяся в ГИС (предназначенная для формирования и ведения перечня и реестра источников доходов бюджетов);
* Информация, содержащаяся в ГИС (сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях);
* Информация, содержащаяся в ГИС (для проведения многомерного анализа финансовой и другой информации, и для решения стратегических задач бюджетного управления).
  + - 1. Основные процессы (бизнес-процессы), для обеспечения которых создана ГИС в сфере финансов:
* Ока­зание го­сударс­твен­ных и му­ници­паль­ных ус­луг (Пред­по­лага­ет ор­га­низа­цию пре­дос­тавле­ния го­сударс­твен­ных и му­ници­паль­ных ус­луг в со­от­ветс­твии с за­коно­датель­ством Рос­сий­ской Фе­дера­ции);
* Ре­али­зация меж­ве­домс­твен­но­го вза­имо­дей­ствия (Ре­али­зу­ет фун­кции ин­форма­ци­он­но­го вза­имо­дей­ствия: с дру­гими ве­домс­тва­ми в рам­ках про­цес­сов ис­полне­ния фун­кций; с цен­тра­лизо­ван­ны­ми ре­ги­ональ­ны­ми и фе­дераль­ны­ми ин­форма­ци­он­ны­ми ре­сур­са­ми);
* Уп­равле­ние и экс­плу­ата­ция ус­луг (Пред­по­лага­ет про­цес­сы пре­дос­тавле­ния, уп­равле­ния и под­дер­жки фун­кци­они­рова­ния ус­луг, ис­поль­зу­емых кли­ен­та­ми или пред­ла­га­емых им (дос­ти­жение тре­бу­емо­го ка­чес­тва ус­луг, обес­пе­чение удов­летво­рен­ности кли­ен­тов па­рамет­ра­ми ра­боты и сто­имос­ти ус­луг));
* Ин­форма­ци­он­но-ана­лити­чес­кая де­ятель­ность (Пред­по­лага­ет: сбор, хра­нение, об­ра­бот­ку и пред­став­ле­ние ин­форма­ции, не­об­хо­димой для под­дер­жки при­нятия уп­равлен­ческих ре­шений; сбор и аг­ре­гацию пер­вичных дан­ных, про­веде­ние эко­номи­чес­ко­го и пред­метно­го ана­лиза и под­го­тов­ку от­четнос­ти; ин­форма­ци­он­ное обес­пе­чение пер­со­нала нор­ма­тив­ной, юри­дичес­кой, опе­ратив­ной, об­зорно-ана­лити­чес­кой, прог­ности­чес­кой ин­форма­цией; сбор, кон­со­лида­цию и об­ра­бот­ку тран­закци­он­ных дан­ных ин­форма­ци­он­ных сис­тем);
* Ад­ми­нис­тра­тив­но-уп­равлен­ческая де­ятель­ность (Пред­по­лага­ет: уп­равле­ние де­ятель­ностью ор­га­низа­ции для дос­ти­жения ее эф­фектив­но­го фун­кци­они­рова­ния; ор­га­низа­цию сов­мес­тной ра­боты кол­лекти­ва ор­га­низа­ции по ре­шению сто­ящих пе­ред ним за­дач);
* Уп­равле­ние фи­нан­са­ми (Ре­али­зу­ет фун­кции по фор­ми­рова­нию и ве­дению бюд­же­та ор­га­низа­ции на оче­ред­ной фи­нан­со­вый год и пла­новый пе­ри­од);
* Пла­ниро­вание бюд­же­та ре­ги­она и ис­полне­ние до­ходов и рас­хо­дов бюд­же­тов субъ­ек­тов, ад­ми­нис­тра­тив­но-тер­ри­тори­аль­ных и му­ници­паль­ных об­ра­зова­ний (Пред­по­лага­ет пла­ниро­вание рас­хо­дов, прог­но­зиро­вание до­ходов, ре­гули­рова­ние меж­бюджет­ных от­но­шений, фор­ми­рова­ние, ве­дение и оцен­ку эф­фектив­ности го­сударс­твен­ных (му­ници­паль­ных) прог­рамм, го­сударс­твен­ных (му­ници­паль­ных) за­даний и пла­нов фи­нан­со­во-хо­зяй­ствен­ной де­ятель­нос­ти, сос­тавле­ние и ис­полне­ние до­ходов и рас­хо­дов бюд­же­тов субъ­ек­тов, ад­ми­нис­тра­тив­но-тер­ри­тори­аль­ных и му­ници­паль­ных об­ра­зова­ний).
  + - 1. Класс защищенности ГИС: 2 («Акт классификации государственной информационной системы в сфере финансов Министерства цифрового развития и связи Курской области ГУПКО «ИЦ «Регион‑Курск» от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_).
      2. Уровень защищенности ПДн: 3 («Акт классификации государственной информационной системы в сфере финансов Министерства цифрового развития и связи Курской области ГУПКО «ИЦ «Регион‑Курск» от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_).
  1. **Состав и архитектура объекта оценки**
     1. Состав ГИС в сфере финансов определен в таблице 3.

Таблица 3 – Состав ГИС в сфере финансов

| №  п/п | Характеристика | Значение характеристики |
| --- | --- | --- |
| 1. | Прог­раммно-аппа­рат­ные средства | Сетевое хранилище данных Dell EMC ME4024 – 1  Сервер – 1 |
| 2. | Об­ще­сис­тем­ное прог­раммное обес­пе­че­ние | Опе­ра­ционные сис­темы:  - Astra Linux |
| 3. | Прик­лад­ное прог­раммное обес­пе­че­ние | - ПК «Бюд­жет-СМАРТ» |
| 4. | Средства за­щи­ты инфор­ма­ции | **Средства крипто­гра­фической защиты ин­фор­ма­ции:**  - Прог­рам­мно-ап­па­рат­ный ком­плекс «ViPNet Coordinator HW 4» (ис­полне­ние HW2000) (Сертифицирующий орган ФСБ России № СФ/124-4156 от 31.10.2021 действителен до 01.06.2024,Сертифицирующий орган ФСБ России № СФ/124-3674 от 12.04.2019 действителен до 31.10.2021,Сертифицирующий орган ФСБ России № СФ/124-3674 от 09.04.2019 действителен до 31.10.2021) |

* + 1. ГИС в сфере финансов представляет собой распределенную систему (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, территориально размещенных в одном или нескольких субъектах РФ и объединенных в единую систему с использованием сетей электросвязи) со следующими характеристиками:
       1. Подключение к сетям электросвязи, включенным в состав единой сети электросвязи Российской Федерации – присутствует, в соответствии с таблицей 4.

Таблица 4 – Подключения к сетям электросвязи

| **№**   1. **п/п** | **Ка­те­гория сети элект­ро­связи** | **Наи­менование оператора связи** | **Цель взаимо­действия с сетью элект­росвязи** | **Способ взаимо­действия с сетью электро­связи** |
| --- | --- | --- | --- | --- |
| 1. | об­ще­го поль­зо­вания | ГУП КО «ИЦ «Ре­ги­он-Курск» | ока­зание ус­луг | Тип доступа проводной, протоколы HTTP, FTP, TCP/IP |

* + - 1. Подключение к информационно-телекоммуникационным сетям Предприятия – отсутствует.
      2. Подключение к информационно-телекоммуникационной сети «Интернет» – отсутствует.
      3. Подключение к информационно-телекоммуникационным сетям иных организаций – отсутствует.
      4. В ГИС в сфере финансов не осуществляется взаимодействие с системами и сетями других организаций.
      5. В ГИС в сфере финансов не осуществляется взаимодействие с другими системами и сетями Предприятия.
      6. К информационным ресурсам ГИС в сфере финансов осуществляется локальный доступ. Особенности локального доступа приведены в таблице 5.

Таблица 5 – Локальный доступ

| Лица, осуществляющие локальный доступ | Цель дос­ту­па | Спо­соб дос­ту­па | Куда осуществляется доступ? |
| --- | --- | --- | --- |
| Сот­руд­ник ор­га­ни­за­ции | Ве­дение ИС | с использованием технологии толстого клиента | Ко всем узлам системы |

* + - 1. К информационным ресурсам ГИС в сфере финансов осуществляется удаленный доступ. Особенности удаленного доступа приведены в таблице 6.

Таблица 6 – Удаленный доступ

| Лица, осуществляющие удаленный доступ | Цель дос­ту­па | Спо­соб дос­ту­па | Куда осуществляется доступ? |
| --- | --- | --- | --- |
| Раз­ра­бот­чи­ки | Об­слу­жива­ние ИС | с использованием технологии толстого клиента | Сервер (Card46), Dell EMC ME4024 |

* + 1. Технологии, используемые в ГИС в сфере финансов отражены в таблице 7.

Таблица 7 – Технологии, используемые в ГИС в сфере финансов

| №  п/п | Технология | Используется / Не используется |
| --- | --- | --- |
| 1. | Съемные носители информации | Не используются |
| 2. | Технология виртуализации | Используются |
| 3. | Технология беспроводного доступа | Не используются |
| 4. | Мобильные технические средства | Не используются |
| 5. | Веб-серверы | Используются |
| 6. | Технология веб-доступа | Не используются |
| 7. | Smart-карты | Не используются |
| 8. | Технологии грид-систем | Не используются |
| 9. | Технологии суперкомпьютерных систем | Не используются |
| 10. | Большие данные | Не используются |
| 11. | Числовое программное оборудование | Не используются |
| 12. | Одноразовые пароли | Не используются |
| 13. | Электронная почта | Не используется |
| 14. | Технология передачи видеоинформации | Не используется |
| 15. | Технология удаленного рабочего стола | Используются |
| 16. | Технология удаленного администрирования | Используются |
| 17. | Технология удаленного внеполосного доступа | Не используются |
| 18. | Технология передачи речи | Не используются |
| 19. | Технология искусственного интеллекта | Не используются |

* + 1. ГИС в сфере финансов функционирует на базе информационно-телекоммуникационной инфраструктуры центра обработки данных (далее – ЦОД). Сведения об используемом ЦОД представлены в таблице 8.

Таблица 8 – Сведения о поставщике вычислительных услуг

| Характеристика | Значение характеристики |
| --- | --- |
| Поставщик вычислительных услуг | ГУП КО «ИЦ «Регион-Курск» |
| Модель предоставления вычислительных услуг | Инфраструктура как услуга |
| Адрес размещения ЦОД | г. Курск, ул. Горького, 65, пом.1 |
| Наименование организации, выдавшей аттестат соответствия ЦОД | – |
| Номер аттестата ЦОД | – |
| Дата выдачи аттестата ЦОД | – |
| Срок действия аттестата ЦОД | – |
| Сведения об оценке угроз безопасности информации поставщиком вычислительных услуг | Поставщик услуг оценил угрозы информации и предоставил результаты такой оценки. Результаты представлены в 51558 |

1. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
   1. В ходе оценки угроз безопасности информации определяются негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.
   2. Негативные последствия определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивает ГИС в сфере финансов, и применительно к нарушению безопасности информации, содержащейся в ГИС в сфере финансов.
   3. На основе анализа исходных данных ГИС в сфере финансов определены негативные последствия, которые приводят к видам рисков (ущерба), представленные в таблице 9.

Таблица 9 – Виды рисков (ущерба) и негативные последствия

| Иден­ти­фи­ка­тор | Не­га­тив­ные пос­ледствия | Вид рис­ка (ущер­ба) |
| --- | --- | --- |
| НП.1 | Раз­гла­шение пер­со­наль­ных дан­ных граж­дан | У1. Ущерб фи­зичес­ко­му ли­цу |
| НП.2 | Неп­ре­дос­тавле­ние го­сударс­твен­ных ус­луг | У3. Ущерб го­сударс­тву в об­ласти обес­пе­чения обо­роны стра­ны, бе­зопас­ности го­сударс­тва и пра­вопо­ряд­ка, а так­же в со­ци­аль­ной, эко­номи­чес­кой, по­лити­чес­кой, эко­логи­чес­кой сфе­рах де­таль­нос­ти |
| НП.3 | На­руше­ние сво­боды, лич­ной неп­ри­кос­но­вен­ности | У1. Ущерб фи­зичес­ко­му ли­цу |
| НП.4 | На­руше­ние неп­ри­кос­но­вен­ности час­тной жиз­ни | У1. Ущерб фи­зичес­ко­му ли­цу |
| НП.5 | На­руше­ние лич­ной, се­мей­ной тай­ны, ут­ра­та чес­ти и доб­ро­го име­ни | У1. Ущерб фи­зичес­ко­му ли­цу |
| НП.6 | На­руше­ние иных прав и сво­бод граж­да­нина, зак­реплен­ных в Кон­сти­туции Рос­сий­ской Фе­дера­ции и фе­дераль­ных за­конах | У1. Ущерб фи­зичес­ко­му ли­цу |
| НП.7 | На­руше­ние кон­фи­ден­ци­аль­нос­ти (утеч­ка) пер­со­наль­ных дан­ных | У1. Ущерб фи­зичес­ко­му ли­цу |
| НП.8 | На­руше­ние за­коно­датель­ства Рос­сий­ской Фе­дера­ции (юри­дичес­кое ли­цо, ин­ди­виду­аль­ный пред­при­нима­тель) | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.9 | По­теря (хи­щение) де­неж­ных средств | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.10 | Не­допо­луче­ние ожи­да­емой (прог­но­зиру­емой) при­были | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.11 | Не­об­хо­димость до­пол­ни­тель­ных (не­зап­ла­ниро­ван­ных) зат­рат на вып­ла­ты штра­фов (не­ус­то­ек) или ком­пенса­ций | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.12 | Не­об­хо­димость до­пол­ни­тель­ных (не­зап­ла­ниро­ван­ных) зат­рат на за­куп­ку то­варов, ра­бот или ус­луг (в том чис­ле за­куп­ка прог­рам­мно­го обес­пе­чения, тех­ни­чес­ких средств, вы­шед­ших из строя, за­мена, нас­трой­ка, ре­монт ука­зан­ных средств) | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.13 | Не­об­хо­димость до­пол­ни­тель­ных (не­зап­ла­ниро­ван­ных) зат­рат на вос­ста­нов­ле­ние де­ятель­нос­ти | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.14 | Ут­ра­та до­верия | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.15 | Не­воз­можность ре­шения за­дач (ре­али­зации фун­кций) или сни­жение эф­фектив­ности ре­шения за­дач (ре­али­зации фун­кций) | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.16 | Не­об­хо­димость из­ме­нения (пе­рес­тро­ения) внут­ренних про­цедур для дос­ти­жения це­лей, ре­шения за­дач (ре­али­зации фун­кций) | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.17 | При­нятие неп­ра­виль­ных ре­шений | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.18 | Прос­той ин­форма­ци­он­ной сис­те­мы или се­ти | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.19 | Утеч­ка кон­фи­ден­ци­аль­ной ин­форма­ции (ком­мерчес­кой тай­ны, сек­ре­тов про­из­водс­тва (ноу-хау) и др.) | У2. Рис­ки юри­дичес­ко­му ли­цу, ин­ди­виду­аль­но­му пред­при­нима­телю, свя­зан­ные с хо­зяй­ствен­ной де­ятель­ностью |
| НП.20 | Прек­ра­щение или на­руше­ние фун­кци­они­рова­ния го­сударс­твен­но­го ор­га­на в час­ти не­выпол­не­ния воз­ло­жен­ной на не­го фун­кции (пол­но­мочия) | У3. Ущерб го­сударс­тву в об­ласти обес­пе­чения обо­роны стра­ны, бе­зопас­ности го­сударс­тва и пра­вопо­ряд­ка, а так­же в со­ци­аль­ной, эко­номи­чес­кой, по­лити­чес­кой, эко­логи­чес­кой сфе­рах де­таль­нос­ти |
| НП.21 | От­сутс­твие дос­ту­па к го­сударс­твен­ной ус­лу­ге | У3. Ущерб го­сударс­тву в об­ласти обес­пе­чения обо­роны стра­ны, бе­зопас­ности го­сударс­тва и пра­вопо­ряд­ка, а так­же в со­ци­аль­ной, эко­номи­чес­кой, по­лити­чес­кой, эко­логи­чес­кой сфе­рах де­таль­нос­ти |
| НП.22 | Сни­жение уров­ня до­хода го­сударс­твен­ной кор­по­рации, го­сударс­твен­ной ор­га­низа­ции или ор­га­низа­ции с го­сударс­твен­ным учас­ти­ем | У3. Ущерб го­сударс­тву в об­ласти обес­пе­чения обо­роны стра­ны, бе­зопас­ности го­сударс­тва и пра­вопо­ряд­ка, а так­же в со­ци­аль­ной, эко­номи­чес­кой, по­лити­чес­кой, эко­логи­чес­кой сфе­рах де­таль­нос­ти |
| НП.23 | Воз­никно­вение ущер­ба бюд­же­там Рос­сий­ской Фе­дера­ции | У3. Ущерб го­сударс­тву в об­ласти обес­пе­чения обо­роны стра­ны, бе­зопас­ности го­сударс­тва и пра­вопо­ряд­ка, а так­же в со­ци­аль­ной, эко­номи­чес­кой, по­лити­чес­кой, эко­логи­чес­кой сфе­рах де­таль­нос­ти |
| НП.24 | Уве­личе­ние ко­личес­тва жа­лоб в ор­га­ны го­сударс­твен­ной влас­ти или ор­га­ны мес­тно­го са­мо­уп­равле­ния | У3. Ущерб го­сударс­тву в об­ласти обес­пе­чения обо­роны стра­ны, бе­зопас­ности го­сударс­тва и пра­вопо­ряд­ка, а так­же в со­ци­аль­ной, эко­номи­чес­кой, по­лити­чес­кой, эко­логи­чес­кой сфе­рах де­таль­нос­ти |

1. Возможные объекты воздействия угроз безопасности информации
   1. В ходе оценки угроз безопасности информации определяются информационные ресурсы и компоненты ГИС в сфере финансов, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, определенным в разделе 4 настоящей Модели угроз, – объектов воздействия.
   2. Объекты воздействия определялись для реальной архитектуры и условий функционирования ГИС в сфере финансов на основе анализа исходных данных и проведенной инвентаризации.
   3. Определение объектов воздействия производилось на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.
   4. В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в таблице 10.

Таблица 10 – 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 |

* 1. Итоговый перечень объектов воздействия со списком возможных видов воздействия на них, реализация которых может привести к негативным последствиям, представлен в таблице 11.

Таблица 11 – Объекты воздействия и виды воздействия

| Негативные последствия | Объекты воздействия | Виды воздействия |
| --- | --- | --- |
| Раз­гла­шение пер­со­наль­ных дан­ных граж­дан | Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | ВВ.2; ВВ.3; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Неп­ре­дос­тавле­ние го­сударс­твен­ных ус­луг | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| На­руше­ние сво­боды, лич­ной неп­ри­кос­но­вен­ности | За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| На­руше­ние неп­ри­кос­но­вен­ности час­тной жиз­ни | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| На­руше­ние лич­ной, се­мей­ной тай­ны, ут­ра­та чес­ти и доб­ро­го име­ни | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| На­руше­ние иных прав и сво­бод граж­да­нина, зак­реплен­ных в Кон­сти­туции Рос­сий­ской Фе­дера­ции и фе­дераль­ных за­конах | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| На­руше­ние кон­фи­ден­ци­аль­нос­ти (утеч­ка) пер­со­наль­ных дан­ных | BIOS/UEFI | ВВ.2; ВВ.3; ВВ.4 |
| Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Мик­ропрог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Объ­ек­ты фай­ло­вой сис­те­мы | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Учет­ные дан­ные поль­зо­вате­ля | ВВ.1; ВВ.2; ВВ.4 |
| На­руше­ние за­коно­датель­ства Рос­сий­ской Фе­дера­ции (юри­дичес­кое ли­цо, ин­ди­виду­аль­ный пред­при­нима­тель) | За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | ВВ.2; ВВ.3; ВВ.4 |
| По­теря (хи­щение) де­неж­ных средств | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Объ­ек­ты фай­ло­вой сис­те­мы | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| Учет­ные дан­ные поль­зо­вате­ля | ВВ.1; ВВ.2; ВВ.4 |
| Не­допо­луче­ние ожи­да­емой (прог­но­зиру­емой) при­были | Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | ВВ.2; ВВ.4 |
| Веб-сер­вер | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Не­об­хо­димость до­пол­ни­тель­ных (не­зап­ла­ниро­ван­ных) зат­рат на вып­ла­ты штра­фов (не­ус­то­ек) или ком­пенса­ций | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Не­об­хо­димость до­пол­ни­тель­ных (не­зап­ла­ниро­ван­ных) зат­рат на за­куп­ку то­варов, ра­бот или ус­луг (в том чис­ле за­куп­ка прог­рам­мно­го обес­пе­чения, тех­ни­чес­ких средств, вы­шед­ших из строя, за­мена, нас­трой­ка, ре­монт ука­зан­ных средств) | BIOS/UEFI | ВВ.2; ВВ.3; ВВ.4 |
| Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | ВВ.2; ВВ.4 |
| Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| Веб-сер­вер | ВВ.2; ВВ.3; ВВ.4 |
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | ВВ.2; ВВ.3; ВВ.4 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Мик­ропрог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | ВВ.2; ВВ.3; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | ВВ.2; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Учет­ные дан­ные поль­зо­вате­ля | ВВ.1; ВВ.2; ВВ.4 |
| Не­об­хо­димость до­пол­ни­тель­ных (не­зап­ла­ниро­ван­ных) зат­рат на вос­ста­нов­ле­ние де­ятель­нос­ти | BIOS/UEFI | ВВ.2; ВВ.3; ВВ.4 |
| Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | ВВ.2; ВВ.4 |
| Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | ВВ.2; ВВ.3; ВВ.4 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | ВВ.2; ВВ.3; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Ут­ра­та до­верия | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Не­воз­можность ре­шения за­дач (ре­али­зации фун­кций) или сни­жение эф­фектив­ности ре­шения за­дач (ре­али­зации фун­кций) | BIOS/UEFI | ВВ.2; ВВ.3; ВВ.4 |
| Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | ВВ.2; ВВ.4 |
| Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| Веб-сер­вер | ВВ.2; ВВ.3; ВВ.4 |
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | ВВ.2; ВВ.3; ВВ.4 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Мик­ропрог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Объ­ек­ты фай­ло­вой сис­те­мы | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | ВВ.2; ВВ.3; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | ВВ.2; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Учет­ные дан­ные поль­зо­вате­ля | ВВ.1; ВВ.2; ВВ.4 |
| Не­об­хо­димость из­ме­нения (пе­рес­тро­ения) внут­ренних про­цедур для дос­ти­жения це­лей, ре­шения за­дач (ре­али­зации фун­кций) | BIOS/UEFI | ВВ.2; ВВ.3; ВВ.4 |
| Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | ВВ.2; ВВ.4 |
| Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| Веб-сер­вер | ВВ.2; ВВ.3; ВВ.4 |
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | ВВ.2; ВВ.3; ВВ.4 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Мик­ропрог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Объ­ек­ты фай­ло­вой сис­те­мы | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | ВВ.2; ВВ.3; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | ВВ.2; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| При­нятие неп­ра­виль­ных ре­шений | Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| Прос­той ин­форма­ци­он­ной сис­те­мы или се­ти | Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Утеч­ка кон­фи­ден­ци­аль­ной ин­форма­ции (ком­мерчес­кой тай­ны, сек­ре­тов про­из­водс­тва (ноу-хау) и др.) | BIOS/UEFI | ВВ.2; ВВ.3; ВВ.4 |
| Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| За­щища­емая ин­форма­ция | ВВ.1; ВВ.2; ВВ.4 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Мик­ропрог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Объ­ек­ты фай­ло­вой сис­те­мы | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Учет­ные дан­ные поль­зо­вате­ля | ВВ.1; ВВ.2; ВВ.4 |
| Прек­ра­щение или на­руше­ние фун­кци­они­рова­ния го­сударс­твен­но­го ор­га­на в час­ти не­выпол­не­ния воз­ло­жен­ной на не­го фун­кции (пол­но­мочия) | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Мик­ропрог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Объ­ек­ты фай­ло­вой сис­те­мы | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | ВВ.2; ВВ.3; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |
| От­сутс­твие дос­ту­па к го­сударс­твен­ной ус­лу­ге | BIOS/UEFI | ВВ.2; ВВ.3; ВВ.4 |
| Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | ВВ.2; ВВ.4 |
| Ба­за дан­ных | ВВ.1; ВВ.2; ВВ.4 |
| Веб-сер­вер | ВВ.2; ВВ.3; ВВ.4 |
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Мик­ропрог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Объ­ек­ты фай­ло­вой сис­те­мы | ВВ.1; ВВ.2; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Се­тевое прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Се­тевой тра­фик | ВВ.1; ВВ.2; ВВ.4 |
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | ВВ.2; ВВ.3; ВВ.4 |
| Сис­темное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Сни­жение уров­ня до­хода го­сударс­твен­ной кор­по­рации, го­сударс­твен­ной ор­га­низа­ции или ор­га­низа­ции с го­сударс­твен­ным учас­ти­ем | Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Прик­ладное прог­рам­мное обес­пе­чение | ВВ.2; ВВ.3; ВВ.4 |
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Воз­никно­вение ущер­ба бюд­же­там Рос­сий­ской Фе­дера­ции | Средс­тво вы­чис­ли­тель­ной тех­ни­ки | ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6 |
| Уве­личе­ние ко­личес­тва жа­лоб в ор­га­ны го­сударс­твен­ной влас­ти или ор­га­ны мес­тно­го са­мо­уп­равле­ния | Веб-сайт | ВВ.1; ВВ.2; ВВ.3; ВВ.4 |
| Се­тевое обо­рудо­вание | ВВ.2; ВВ.3; ВВ.4; ВВ.6 |
| Средс­тво за­щиты ин­форма­ции | ВВ.2; ВВ.3; ВВ.4 |

1. Источники угроз безопасности информации
   1. **Антропогенные источники**
      1. В ходе оценки угроз безопасности информации определяются возможные антропогенные 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 ГИС в сфере финансов, – актуальные нарушители.
      2. Процесс определения актуальных нарушителей включал:
         1. 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), представленных в таблице 12.

Таблица 12 – 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;  Срыв зак­лю­чения меж­ду­народ­ных до­гово­ров;  Соз­да­ние внут­ри­поли­тичес­ко­го кри­зиса | ­Це­­ли не пред­­по­­лага­­ют по­­тен­­ци­­аль­­ное 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 |
| 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 ма­тери­аль­ной 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 или 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 или 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 или 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 или 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 |

* + - 1. Определение характеристик (категория нарушителя и уровень возможности по реализации угроз безопасности информации) возможных нарушителей.
      2. Оценка возможности привлечения (вхождения в сговор) одними нарушителями других (в том числе обладающих привилегированными правами доступа).
      3. Сопоставление возможных нарушителей и их целей реализации угроз безопасности информации с возможными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз безопасности информации (Приложение № 2). По результатам сопоставления определяются актуальные нарушители по следующему принципу: нарушитель признается актуальным, если возможные цели реализации нарушителем угроз безопасности информации могут привести к определенным для ГИС в сфере финансов негативным последствиям и соответствующим рискам (видам ущерба).
    1. Итоговые характеристики возможных нарушителей представлены в таблице 13.

Таблица 13 – Характеристики возможных нарушителей

| №  п/п | Возможный вид нарушителя | Категория | Уровень возможностей | Актуальность |
| --- | --- | --- | --- | --- |
| 1. | Тер­ро­рис­ти­чес­кие, экс­тре­мист­ские груп­пи­ров­ки | Внешний | Н3. Нарушитель, обладающий средними возможностями | Да |
| 2. | Прес­тупные груп­пы (кри­миналь­ные струк­ту­ры) | Внешний | Н2. Нарушитель, обладающий базовыми повышенными возможностями | Да |
| 3. | От­дель­ные фи­зичес­кие ли­ца (ха­керы) | Внешний | Н1. Нарушитель, обладающий базовыми возможностями | Да |
| 4. | Кон­ку­риру­ющие ор­га­низа­ции | Внешний | Н2. Нарушитель, обладающий базовыми повышенными возможностями | Да |
| 5. | Раз­ра­бот­чи­ки прог­рам­мных, прог­рам­мно-ап­па­рат­ных средств | Внутренний | Н3. Нарушитель, обладающий средними возможностями | Да |
| 6. | Ли­ца, обес­пе­чива­ющие пос­тавку прог­рам­мных, прог­рам­мно-ап­па­рат­ных средств, обес­пе­чива­ющих сис­тем | Внешний | Н1. Нарушитель, обладающий базовыми возможностями | Да |
| 7. | Пос­тавщи­ки вы­чис­ли­тель­ных ус­луг, ус­луг свя­зи | Внутренний | Н2. Нарушитель, обладающий базовыми повышенными возможностями | Да |
| 8. | Ли­ца, прив­ле­ка­емые для ус­та­нов­ки, нас­трой­ки, ис­пы­таний, пус­ко­нала­доч­ных и иных ви­дов ра­бот | Внутренний | Н2. Нарушитель, обладающий базовыми повышенными возможностями | Да |
| 9. | Ли­ца, обес­пе­чива­ющие фун­кци­они­рова­ние сис­тем и се­тей или обес­пе­чива­ющие сис­те­мы опе­рато­ра | Внутренний | Н1. Нарушитель, обладающий базовыми возможностями | Да |
| 10. | Ав­то­ризо­ван­ные поль­зо­вате­ли сис­тем и се­тей | Внутренний | Н1. Нарушитель, обладающий базовыми возможностями | Да |
| 11. | Сис­темные ад­ми­нис­тра­торы и ад­ми­нис­тра­торы бе­зопас­ности | Внутренний | Н2. Нарушитель, обладающий базовыми повышенными возможностями | Да |
| 12. | Быв­шие (уво­лен­ные) ра­бот­ни­ки (поль­зо­вате­ли) | Внешний | Н1. Нарушитель, обладающий базовыми возможностями | Да |

* + 1. Категория нарушителя определяется исходя из следующих принципов:
* внешний нарушитель – если нарушитель не имеет прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам ГИС в сфере финансов, требующим авторизации;
* внутренний нарушитель – если нарушитель имеет права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам ГИС в сфере финансов. К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам ГИС в сфере финансов.
  + 1. Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.
    2. Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителя по реализации угроз безопасности информации.
    3. Уровень возможности нарушителя определяется исходя из следующих принципов:
* нарушитель, обладающий базовыми возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов;
* нарушитель, обладающий базовыми повышенными возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;
* нарушитель, обладающий средними возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе на выявленные им неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;
* нарушитель, обладающий высокими возможностями по реализации угроз безопасности информации – если имеет практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.
  + 1. Подробное описание уровней возможностей нарушителей по реализации угроз безопасности информации приведено в Приложении № 3.

1. Способы реализации (возникновения) угроз безопасности информации
   1. В ходе оценки угроз безопасности информации определяются возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в ГИС в сфере финансов, – актуальные способы реализации (возникновения) угроз безопасности информации.
   2. Процесс определения актуальных способов реализации (возникновения) угроз безопасности информации включал:
      1. Составление перечня рассматриваемых (возможных) способов реализации угроз безопасности. Перечень возможных способов реализации угроз безопасности информации представлен в таблице 14.

Таблица 14 – 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 программного обеспечения |
| СР.3 | Использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств |
| СР.4 | Установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства |
| СР.5 | Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных |
| СР.6 | Перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| СР.7 | Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| СР.8 | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию) |
| СР.9 | Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств |
| СР.10 | Перехват трафика сети передачи данных |
| СР.11 | Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации |
| СР.12 | Реализация атак типа "отказ в обслуживании" в отношении технических средств, программного обеспечения и каналов передачи данных |

* + 1. Определение интерфейсов объектов воздействия, определенных в соответствии с разделом 5 настоящей Модели угроз. Интерфейсы объектов воздействия определялись на основе изучения и анализа данных:
* об архитектуре, составе и условиях функционирования ГИС в сфере финансов;
* о группах пользователей ГИС в сфере финансов, их типов доступа и уровней полномочий.
  + 1. Определение наличия у актуальных нарушителей возможности доступа к интерфейсам объектов воздействия.
    2. Определение актуальных способов реализации (возникновения) угроз безопасности информации актуальным нарушителем через доступные ему интерфейсы объектов воздействия.
  1. 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 15.

Таблица 15 – 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) |
| --- | --- | --- | --- | --- |
| Тер­ро­рис­ти­чес­кие, экс­тре­мист­ские груп­пи­ров­ки | Внеш­ний | Веб-сайт | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Веб-сер­вер | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.10 |
|
| За­щища­емая ин­форма­ция | Дос­туп к об­лачной сис­те­ме | СР.1; СР.9 |
|
| Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | Поль­зо­вате­ли | СР.1 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Объ­ек­ты фай­ло­вой сис­те­мы | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.4; СР.9 |
|
|
| Се­тевое обо­рудо­вание | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.12 |
|
| Се­тевое прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.12 |
|
|
| Се­тевой тра­фик | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Сис­темное прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2 |
|
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1 |
| 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.9; СР.12 |
|
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Прес­тупные груп­пы (кри­миналь­ные струк­ту­ры) | Внеш­ний | Веб-сайт | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Веб-сер­вер | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.10 |
|
| За­щища­емая ин­форма­ция | Дос­туп к об­лачной сис­те­ме | СР.1; СР.9 |
|
| Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | Поль­зо­вате­ли | СР.1 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Объ­ек­ты фай­ло­вой сис­те­мы | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.4; СР.9 |
|
|
| Се­тевое обо­рудо­вание | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.12 |
|
| Се­тевое прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.12 |
|
|
| Се­тевой тра­фик | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Сис­темное прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2 |
|
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1 |
| 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.9; СР.12 |
|
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| От­дель­ные фи­зичес­кие ли­ца (ха­керы) | Внеш­ний | Веб-сайт | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Веб-сер­вер | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.10 |
|
| За­щища­емая ин­форма­ция | Дос­туп к об­лачной сис­те­ме | СР.1; СР.9 |
|
| Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | Поль­зо­вате­ли | СР.1 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Объ­ек­ты фай­ло­вой сис­те­мы | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.4; СР.9 |
|
|
| Се­тевое обо­рудо­вание | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.12 |
|
| Се­тевое прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.12 |
|
|
| Се­тевой тра­фик | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Сис­темное прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2 |
|
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1 |
| 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.9; СР.12 |
|
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Кон­ку­риру­ющие ор­га­низа­ции | Внеш­ний | Веб-сайт | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Веб-сер­вер | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.10 |
|
| За­щища­емая ин­форма­ция | Дос­туп к об­лачной сис­те­ме | СР.1; СР.9 |
|
| Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | Поль­зо­вате­ли | СР.1 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Объ­ек­ты фай­ло­вой сис­те­мы | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.4; СР.9 |
|
|
| Се­тевое обо­рудо­вание | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.12 |
|
| Се­тевое прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.12 |
|
|
| Се­тевой тра­фик | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Сис­темное прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2 |
|
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1 |
| 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.9; СР.12 |
|
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ли­ца, обес­пе­чива­ющие пос­тавку прог­рам­мных, прог­рам­мно-ап­па­рат­ных средств, обес­пе­чива­ющих сис­тем | Внеш­ний | BIOS/UEFI | Фи­зичес­кий дос­туп к ап­па­рат­но­му обес­пе­чению BIOS | СР.8; СР.9; СР.11 |
|
|
| Кон­соль уп­равле­ния BIOS/UEFI | СР.1; СР.9 |
|
| За­щища­емая ин­форма­ция | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.9; СР.11 |
|
|
|
| Се­тевое обо­рудо­вание | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.4; СР.5; СР.8; СР.9; СР.11 |
|
|
|
|
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.9; СР.11 |
|
|
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | Кон­соль уп­равле­ния сис­те­мой под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.9 |
|
| Фи­зичес­кий дос­туп к тех­ни­чес­ким средс­твам сис­те­мы под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.11 |
|
| Средс­тво за­щиты ин­форма­ции | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам за­щиты ин­форма­ции | СР.8; СР.11 |
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.11 |
|
| Пос­тавщи­ки вы­чис­ли­тель­ных ус­луг, ус­луг свя­зи | Внут­ренний | Веб-сайт | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Веб-сер­вер | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| За­щища­емая ин­форма­ция | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Объ­ек­ты фай­ло­вой сис­те­мы | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.4; СР.9 |
|
|
| Се­тевое обо­рудо­вание | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.12 |
|
| Се­тевое прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.12 |
|
|
| Се­тевой тра­фик | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ли­ца, прив­ле­ка­емые для ус­та­нов­ки, нас­трой­ки, ис­пы­таний, пус­ко­нала­доч­ных и иных ви­дов ра­бот | Внут­ренний | BIOS/UEFI | Ме­ханизм об­новле­ния BIOS/UEFI | СР.1; СР.2; СР.9 |
|
|
| Фи­зичес­кий дос­туп к ап­па­рат­но­му обес­пе­чению BIOS | СР.8; СР.9; СР.11 |
|
|
| Кон­соль уп­равле­ния BIOS/UEFI | СР.1; СР.9 |
|
| Веб-сайт | Веб-ин­терфейс сис­те­мы ад­ми­нис­три­рова­ния Веб-сай­та | СР.9 |
| Ба­за дан­ных | Слу­жеб­ные прог­раммы ко­ман­дной стро­ки СУБД | СР.9 |
| Поль­зо­ватель­ский ин­терфейс СУБД | СР.9 |
| Веб-сер­вер | Слу­жеб­ные прог­раммы ко­ман­дной стро­ки для уп­равле­ния Веб-сер­ве­ром | СР.8; СР.9 |
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Дос­туп к сис­те­ме уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой | СР.1; СР.8; СР.9 |
|
|
| Дос­туп к ги­пер­ви­зору | СР.1; СР.2; СР.8; СР.9 |
|
|
|
| Вир­ту­аль­ные ка­налы пе­реда­чи дан­ных | СР.10 |
| Дос­туп к вир­ту­аль­ным ус­трой­ствам хра­нения дан­ных и (или) вир­ту­аль­ным дис­кам | СР.1; СР.9 |
|
| Дос­туп к вир­ту­аль­ным ус­трой­ствам | СР.1; СР.2; СР.9 |
|
|
| Дос­туп к об­ра­зам вир­ту­аль­ных ма­шин | СР.1; СР.9 |
|
| За­щища­емая ин­форма­ция | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.7; СР.11 |
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.9; СР.11 |
|
|
|
| Вир­ту­аль­ные ка­налы пе­реда­чи дан­ных | СР.10 |
| Дос­туп к вир­ту­аль­ным ус­трой­ствам хра­нения дан­ных и (или) вир­ту­аль­ным дис­кам | СР.9 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | Средс­тва цен­тра­лизо­ван­но­го уп­равле­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми | СР.9 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.8; СР.9 |
|
| Че­рез фун­кции вво­да-вы­вода низ­ко­го уров­ня (пря­мого дос­ту­па) | СР.8 |
| Фи­зичес­кий дос­туп к ма­шин­ным но­сите­лям ин­форма­ции | СР.11 |
| Мик­ропрог­рам­мное обес­пе­чение | Кон­соль уп­равле­ния мик­ропрог­рам­мным обес­пе­чени­ем | СР.1; СР.9 |
|
| Ме­ханизм об­новле­ния мик­ропрог­рам­мно­го обес­пе­чения | СР.2; СР.4 |
|
| Прик­ладное прог­рам­мное обес­пе­чение | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.8; СР.9 |
|
|
|
| Се­тевое обо­рудо­вание | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.4; СР.5; СР.8; СР.9; СР.11 |
|
|
|
|
| Се­тевое прог­рам­мное обес­пе­чение | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.5; СР.8; СР.9 |
|
|
|
|
| Се­тевой тра­фик | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | Уда­лен­ные ка­налы ад­ми­нис­три­рова­ния сис­те­мы под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.9 |
|
| Кон­соль уп­равле­ния сис­те­мой под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.9 |
|
| Фи­зичес­кий дос­туп к тех­ни­чес­ким средс­твам сис­те­мы под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.11 |
|
| Сис­темное прог­рам­мное обес­пе­чение | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.2; СР.4; СР.8; СР.9 |
|
|
|
|
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.9; СР.11 |
|
|
| Поль­зо­ватель­ский ин­терфейс ра­боты с сис­темным прог­рам­мным обес­пе­чени­ем | СР.1; СР.2; СР.9 |
|
|
| Ин­терфей­сы под­клю­чения съ­ем­ных ма­шин­ных но­сите­лей ин­форма­ции | СР.1; СР.2 |
|
| Средс­тво за­щиты ин­форма­ции | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам за­щиты ин­форма­ции | СР.8; СР.11 |
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.9 |
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы уда­лен­но­го ад­ми­нис­три­рова­ния уз­ла вы­чис­ли­тель­ной се­ти | СР.1 |
| Гра­фичес­кий ин­терфейс ло­каль­но­го вза­имо­дей­ствия поль­зо­вате­ля с уз­лом вы­чис­ли­тель­ной се­ти | СР.2; СР.9 |
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.11 |
|
| Учет­ные дан­ные поль­зо­вате­ля | Дос­туп к объ­ек­там фай­ло­вой сис­те­мы, со­дер­жа­щим учет­ные дан­ные поль­зо­вате­ля | СР.1; СР.9 |
|
| Ли­ца, обес­пе­чива­ющие фун­кци­они­рова­ние сис­тем и се­тей или обес­пе­чива­ющие сис­те­мы опе­рато­ра | Внут­ренний | BIOS/UEFI | Кон­соль уп­равле­ния BIOS/UEFI | СР.1; СР.9 |
|
| Фи­зичес­кий дос­туп к ап­па­рат­но­му обес­пе­чению BIOS | СР.8; СР.9; СР.11 |
|
|
| Ме­ханизм об­новле­ния BIOS/UEFI | СР.1; СР.2; СР.9 |
|
|
| За­щища­емая ин­форма­ция | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.7; СР.11 |
|
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | Фи­зичес­кий дос­туп к ма­шин­ным но­сите­лям ин­форма­ции | СР.11 |
| Се­тевое обо­рудо­вание | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.4; СР.5; СР.8; СР.9; СР.11 |
|
|
|
|
| Объ­ек­ты фай­ло­вой сис­те­мы | Фи­зичес­кий дос­туп к ма­шин­ным но­сите­лям ин­форма­ции | СР.1; СР.4; СР.8; СР.11 |
|
|
|
| Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | Уда­лен­ные ка­налы ад­ми­нис­три­рова­ния сис­те­мы под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.9 |
|
| Фи­зичес­кий дос­туп к тех­ни­чес­ким средс­твам сис­те­мы под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.11 |
|
| Кон­соль уп­равле­ния сис­те­мой под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | СР.1; СР.9 |
|
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.9; СР.11 |
|
|
| Средс­тво за­щиты ин­форма­ции | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам за­щиты ин­форма­ции | СР.8; СР.11 |
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.11 |
|
| Ав­то­ризо­ван­ные поль­зо­вате­ли сис­тем и се­тей | Внут­ренний | BIOS/UEFI | Фи­зичес­кий дос­туп к ап­па­рат­но­му обес­пе­чению BIOS | СР.8; СР.9; СР.11 |
|
|
| Веб-сайт | Веб-ин­терфейс поль­зо­вате­ля Веб-сай­та | СР.1; СР.2 |
|
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.10 |
| Ба­за дан­ных | Прик­ладное при­ложе­ние, ис­поль­зу­ющее ба­зу дан­ных | СР.1 |
| Веб-сер­вер | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.2 |
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Вир­ту­аль­ные ка­налы пе­реда­чи дан­ных | СР.10 |
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.10 |
|
| Дос­туп к вир­ту­аль­ным ма­шинам | СР.1; СР.2 |
|
| За­щища­емая ин­форма­ция | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.9; СР.11 |
|
|
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.7; СР.11 |
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.10 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | Фи­зичес­кий дос­туп к ма­шин­ным но­сите­лям ин­форма­ции | СР.11 |
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.8; СР.9 |
|
| Мик­ропрог­рам­мное обес­пе­чение | Кон­соль уп­равле­ния мик­ропрог­рам­мным обес­пе­чени­ем | СР.1; СР.9 |
|
| Объ­ек­ты фай­ло­вой сис­те­мы | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.4; СР.9 |
|
|
| Фи­зичес­кий дос­туп к ма­шин­ным но­сите­лям ин­форма­ции | СР.1; СР.4; СР.8; СР.11 |
|
|
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.8; СР.9 |
|
|
|
| Прик­ладное прог­рам­мное обес­пе­чение | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.12 |
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.8; СР.9 |
|
|
|
| Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.9 |
|
| Се­тевое обо­рудо­вание | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.12 |
|
| Се­тевое прог­рам­мное обес­пе­чение | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.5; СР.8; СР.9 |
|
|
|
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.9; СР.12 |
|
|
| Сис­темное прог­рам­мное обес­пе­чение | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.2 |
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.2; СР.4; СР.8; СР.9 |
|
|
|
|
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.2 |
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.9; СР.11 |
|
|
| Поль­зо­ватель­ский ин­терфейс ра­боты с сис­темным прог­рам­мным обес­пе­чени­ем | СР.1; СР.2; СР.9 |
|
|
| Ин­терфей­сы под­клю­чения съ­ем­ных ма­шин­ных но­сите­лей ин­форма­ции | СР.1; СР.2 |
|
| Средс­тво за­щиты ин­форма­ции | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.9; СР.12 |
|
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.9 |
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам за­щиты ин­форма­ции | СР.8; СР.11 |
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.2; СР.12 |
|
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.11 |
|
| Гра­фичес­кий ин­терфейс ло­каль­но­го вза­имо­дей­ствия поль­зо­вате­ля с уз­лом вы­чис­ли­тель­ной се­ти | СР.2; СР.9 |
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.10 |
| Дос­туп к объ­ек­там фай­ло­вой сис­те­мы, со­дер­жа­щим учет­ные дан­ные поль­зо­вате­ля | СР.1; СР.9 |
|
| Сис­темные ад­ми­нис­тра­торы и ад­ми­нис­тра­торы бе­зопас­ности | Внут­ренний | BIOS/UEFI | Кон­соль уп­равле­ния BIOS/UEFI | СР.1; СР.9 |
|
| Фи­зичес­кий дос­туп к ап­па­рат­но­му обес­пе­чению BIOS | СР.8; СР.9; СР.11 |
|
|
| Ме­ханизм об­новле­ния BIOS/UEFI | СР.1; СР.2; СР.9 |
|
|
| Веб-сайт | Веб-ин­терфейс сис­те­мы ад­ми­нис­три­рова­ния Веб-сай­та | СР.9 |
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.10 |
| Ба­за дан­ных | Поль­зо­ватель­ский ин­терфейс СУБД | СР.9 |
| Слу­жеб­ные прог­раммы ко­ман­дной стро­ки СУБД | СР.9 |
| Веб-сер­вер | Слу­жеб­ные прог­раммы ко­ман­дной стро­ки для уп­равле­ния Веб-сер­ве­ром | СР.8; СР.9 |
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Дос­туп к сис­те­ме уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой | СР.1; СР.8; СР.9 |
|
|
| Дос­туп к вир­ту­аль­ным ма­шинам | СР.1; СР.2 |
|
| Дос­туп к об­ра­зам вир­ту­аль­ных ма­шин | СР.1; СР.9 |
|
| Дос­туп к вир­ту­аль­ным ус­трой­ствам | СР.1; СР.2; СР.9 |
|
|
| Дос­туп к вир­ту­аль­ным ус­трой­ствам хра­нения дан­ных и (или) вир­ту­аль­ным дис­кам | СР.1; СР.9 |
|
| Вир­ту­аль­ные ка­налы пе­реда­чи дан­ных | СР.10 |
| Дос­туп к ги­пер­ви­зору | СР.1; СР.2; СР.8; СР.9 |
|
|
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.10 |
|
| За­щища­емая ин­форма­ция | Дос­туп к вир­ту­аль­ным ус­трой­ствам хра­нения дан­ных и (или) вир­ту­аль­ным дис­кам | СР.9 |
| Вир­ту­аль­ные ка­налы пе­реда­чи дан­ных | СР.10 |
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.9; СР.11 |
|
|
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.7; СР.11 |
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.10 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | Средс­тва цен­тра­лизо­ван­но­го уп­равле­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми | СР.9 |
| Про­цесс соз­да­ния (мо­дер­ни­зации) ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мы | СР.4; СР.8; СР.9 |
|
|
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | Ме­ханизм пе­рено­са ин­фраструк­ту­ры в об­ла­ко или сме­ны про­вай­де­ра об­лачных ус­луг | СР.9 |
| Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.8; СР.9 |
|
| Че­рез фун­кции вво­да-вы­вода низ­ко­го уров­ня (пря­мого дос­ту­па) | СР.8 |
| Фи­зичес­кий дос­туп к ма­шин­ным но­сите­лям ин­форма­ции | СР.11 |
| Мик­ропрог­рам­мное обес­пе­чение | Кон­соль уп­равле­ния мик­ропрог­рам­мным обес­пе­чени­ем | СР.1; СР.9 |
|
| Ме­ханизм об­новле­ния мик­ропрог­рам­мно­го обес­пе­чения | СР.2; СР.4 |
|
| Объ­ек­ты фай­ло­вой сис­те­мы | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.8; СР.9 |
|
|
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.4; СР.9 |
|
|
| Фи­зичес­кий дос­туп к ма­шин­ным но­сите­лям ин­форма­ции | СР.1; СР.4; СР.8; СР.11 |
|
|
|
| Прик­ладное прог­рам­мное обес­пе­чение | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.12 |
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.8; СР.9 |
|
|
|
| Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.9 |
|
| Ка­нал уда­лен­но­го ад­ми­нис­три­рова­ния СКЗИ | СР.1 |
| Се­тевое обо­рудо­вание | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.12 |
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.4; СР.5; СР.8; СР.9; СР.11 |
|
|
|
|
| Се­тевое прог­рам­мное обес­пе­чение | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.5; СР.8; СР.9 |
|
|
|
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.9; СР.12 |
|
|
| Се­тевой тра­фик | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Сис­темное прог­рам­мное обес­пе­чение | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.2 |
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.2; СР.4; СР.8; СР.9 |
|
|
|
|
| Средс­тво вы­чис­ли­тель­ной тех­ни­ки | Ин­терфей­сы под­клю­чения съ­ем­ных ма­шин­ных но­сите­лей ин­форма­ции | СР.1; СР.2 |
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.2 |
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.9; СР.11 |
|
|
| Поль­зо­ватель­ский ин­терфейс ра­боты с сис­темным прог­рам­мным обес­пе­чени­ем | СР.1; СР.2; СР.9 |
|
|
| Средс­тво за­щиты ин­форма­ции | Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам за­щиты ин­форма­ции | СР.8; СР.11 |
|
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.9; СР.12 |
|
|
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.9 |
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Гра­фичес­кий ин­терфейс ло­каль­но­го вза­имо­дей­ствия поль­зо­вате­ля с уз­лом вы­чис­ли­тель­ной се­ти | СР.2; СР.9 |
|
| Ка­налы уда­лен­но­го ад­ми­нис­три­рова­ния уз­ла вы­чис­ли­тель­ной се­ти | СР.1 |
| Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.1; СР.2; СР.12 |
|
|
| Фи­зичес­кий дос­туп к прог­рам­мно-ап­па­рат­ным средс­твам об­ра­бот­ки ин­форма­ции | СР.8; СР.11 |
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи уз­лов ло­каль­ной вы­чис­ли­тель­ной се­ти | СР.10 |
| Дос­туп к объ­ек­там фай­ло­вой сис­те­мы, со­дер­жа­щим учет­ные дан­ные поль­зо­вате­ля | СР.1; СР.9 |
|
| Быв­шие (уво­лен­ные) ра­бот­ни­ки (поль­зо­вате­ли) | Внеш­ний | Веб-сайт | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| XML-схе­ма, пе­реда­ва­емая меж­ду кли­ен­том и сер­ве­ром | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Веб-сер­вер | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.10 |
|
| За­щища­емая ин­форма­ция | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Объ­ек­ты фай­ло­вой сис­те­мы | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.4; СР.9 |
|
|
| Се­тевое прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.12 |
|
|
| Се­тевой тра­фик | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.9; СР.10; СР.12 |
|
|
|
| Сис­темное прог­рам­мное обес­пе­чение | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2 |
|
| Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1 |
| 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.9; СР.12 |
|
|
| Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.1; СР.2; СР.12 |
|
|
| Учет­ные дан­ные поль­зо­вате­ля | Ка­налы свя­зи с внеш­ни­ми ин­форма­ци­он­но-те­леком­му­ника­ци­он­ны­ми се­тями | СР.10 |
| Раз­ра­бот­чи­ки прог­рам­мных, прог­рам­мно-ап­па­рат­ных средств | Внут­ренний | Ба­за дан­ных | Прик­ладное при­ложе­ние, ис­поль­зу­ющее ба­зу дан­ных | СР.1 |
| За­щища­емая ин­форма­ция | Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.4; СР.9; СР.11 |
|
|
|
| Мик­ропрог­рам­мное обес­пе­чение | Ус­трой­ства, пред­назна­чен­ные для за­писи/счи­тыва­ния ин­форма­ции с ПЗУ (прог­рамма­торы) | СР.8; СР.9 |
|
| Тер­ро­рис­ти­чес­кие, экс­тре­мист­ские груп­пи­ров­ки | Внеш­ний | Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | Ка­нал уда­лен­но­го ад­ми­нис­три­рова­ния СКЗИ | СР.1 |
| Раз­ра­бот­чи­ки прог­рам­мных, прог­рам­мно-ап­па­рат­ных средств | Внут­ренний | Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | Ка­нал уда­лен­но­го ад­ми­нис­три­рова­ния СКЗИ | СР.1 |
| Дос­туп че­рез средс­тва вы­чис­ли­тель­ной тех­ни­ки | СР.1; СР.9 |
|
| Прес­тупные груп­пы (кри­миналь­ные струк­ту­ры) | Внеш­ний | BIOS/UEFI | Ме­ханизм об­новле­ния BIOS/UEFI | СР.1; СР.2; СР.9 |
|
|
| Кон­соль уп­равле­ния BIOS/UEFI | СР.1; СР.9 |
|
| Кон­ку­риру­ющие ор­га­низа­ции | Внеш­ний | BIOS/UEFI | Кон­соль уп­равле­ния BIOS/UEFI | СР.1; СР.9 |
|
| Ме­ханизм об­новле­ния BIOS/UEFI | СР.1; СР.2; СР.9 |
|
|
| Тер­ро­рис­ти­чес­кие, экс­тре­мист­ские груп­пи­ров­ки | Внеш­ний | BIOS/UEFI | Кон­соль уп­равле­ния BIOS/UEFI | СР.1; СР.9 |
|
| Ме­ханизм об­новле­ния BIOS/UEFI | СР.1; СР.2; СР.9 |
|
|

1. Актуальные угрозы безопасности информации
   1. В ходе оценки угроз безопасности информации определяются возможные угрозы безопасности информации и производится их оценка на актуальность для ГИС в сфере финансов – актуальные угрозы безопасности информации.
   2. Процесс определения актуальных угроз безопасности информации включал:
      1. 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:

УБИi = [нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия]

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

Перечень исключенных из исходного перечня угроз безопасности информации представлен в Приложении № 4.

* + 1. Оценку возможных угроз на предмет актуальности по следующему принципу: угроза признается актуальной, если имеется хотя бы один сценарий реализации угрозы безопасности информации.

Сценарии определяются для соответствующих способов реализации угроз безопасности информации.

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 и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации представлен в Приложении № 5.

* 1. По результатам оценки возможных угроз безопасности выявлено актуальных угроз: 147. Итоговый перечень актуальных угроз безопасности информации представлен в таблице 16. Выводы об актуальности угроз безопасности информации с приведенными сценариями их реализации представлены в Приложении № 6.

Таблица 16 – Актуальные угрозы безопасности информации

| Иден­ти­фи­ка­тор угрозы | Наименование угрозы |
| --- | --- |
| УБИ.003 | Уг­ро­за ис­поль­зо­вания сла­бос­тей крип­тогра­фичес­ких ал­го­рит­мов и у­яз­ви­мос­тей в прог­рам­мном обес­пе­чении их ре­али­зации |
| УБИ.004 | Уг­ро­за ап­па­рат­но­го сбро­са па­роля BIOS |
| УБИ.006 | Уг­ро­за внед­ре­ния ко­да или дан­ных |
| УБИ.007 | Уг­ро­за воз­дей­ствия на прог­раммы с вы­соки­ми при­виле­ги­ями |
| УБИ.008 | Уг­ро­за вос­ста­нов­ле­ния и/или пов­торно­го ис­поль­зо­вания а­утен­ти­фика­ци­он­ной ин­форма­ции |
| УБИ.009 | Уг­ро­за вос­ста­нов­ле­ния пре­дыду­щей у­яз­ви­мой вер­сии BIOS |
| УБИ.010 | Уг­ро­за вы­хода про­цес­са за пре­делы вир­ту­аль­ной ма­шины |
| УБИ.012 | Уг­ро­за дес­трук­тивно­го из­ме­нения кон­фи­гура­ции/сре­ды ок­ру­жения прог­рамм |
| УБИ.013 | Уг­ро­за дес­трук­тивно­го ис­поль­зо­вания дек­ла­риро­ван­но­го фун­кци­она­ла BIOS |
| УБИ.014 | Уг­ро­за дли­тель­но­го удер­жа­ния вы­чис­ли­тель­ных ре­сур­сов поль­зо­вате­лями |
| УБИ.015 | Уг­ро­за дос­ту­па к за­щища­емым фай­лам с ис­поль­зо­вани­ем об­ходно­го пу­ти |
| УБИ.016 | Уг­ро­за дос­ту­па к ло­каль­ным фай­лам сер­ве­ра при по­мощи URL |
| УБИ.018 | Уг­ро­за заг­рузки неш­татной опе­раци­он­ной сис­те­мы |
| УБИ.019 | Уг­ро­за за­раже­ния DNS-ке­ша |
| УБИ.022 | Уг­ро­за из­бы­точ­но­го вы­деле­ния опе­ратив­ной па­мяти |
| УБИ.023 | Уг­ро­за из­ме­нения ком­по­нен­тов ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мы |
| УБИ.025 | Уг­ро­за из­ме­нения сис­темных и гло­баль­ных пе­ремен­ных |
| УБИ.027 | Уг­ро­за ис­ка­жения вво­димой и вы­води­мой на пе­рифе­рий­ные ус­трой­ства ин­форма­ции |
| УБИ.028 | Уг­ро­за ис­поль­зо­вания аль­тер­на­тив­ных пу­тей дос­ту­па к ре­сур­сам |
| УБИ.030 | Уг­ро­за ис­поль­зо­вания ин­форма­ции иден­ти­фика­ции/а­утен­ти­фика­ции, за­дан­ной по умол­ча­нию |
| УБИ.031 | Уг­ро­за ис­поль­зо­вания ме­ханиз­мов ав­то­риза­ции для по­выше­ния при­виле­гий |
| УБИ.032 | Уг­ро­за ис­поль­зо­вания под­дель­ных циф­ро­вых под­пи­сей BIOS |
| УБИ.033 | Уг­ро­за ис­поль­зо­вания сла­бос­тей ко­диро­вания вход­ных дан­ных |
| УБИ.034 | Уг­ро­за ис­поль­зо­вания сла­бос­тей про­токо­лов се­тево­го/ло­каль­но­го об­ме­на дан­ны­ми |
| УБИ.036 | Уг­ро­за ис­сле­дова­ния ме­ханиз­мов ра­боты прог­раммы |
| УБИ.037 | Уг­ро­за ис­сле­дова­ния при­ложе­ния че­рез от­чё­ты об ошиб­ках |
| УБИ.039 | Уг­ро­за ис­черпа­ния за­паса клю­чей, не­об­хо­димых для об­новле­ния BIOS |
| УБИ.041 | Уг­ро­за меж­сай­то­вого скрип­тинга |
| УБИ.042 | Уг­ро­за меж­сай­то­вой под­делки зап­ро­са |
| УБИ.044 | Уг­ро­за на­руше­ния изо­ляции поль­зо­ватель­ских дан­ных внут­ри вир­ту­аль­ной ма­шины |
| УБИ.045 | Уг­ро­за на­руше­ния изо­ляции сре­ды ис­полне­ния BIOS |
| УБИ.046 | Уг­ро­за на­руше­ния про­цеду­ры а­утен­ти­фика­ции субъ­ек­тов вир­ту­аль­но­го ин­форма­ци­он­но­го вза­имо­дей­ствия |
| УБИ.048 | Уг­ро­за на­руше­ния тех­но­логии об­ра­бот­ки ин­форма­ции пу­тём не­сан­кци­они­рован­но­го вне­сения из­ме­нений в об­ра­зы вир­ту­аль­ных ма­шин |
| УБИ.049 | Уг­ро­за на­руше­ния це­лос­тнос­ти дан­ных ке­ша |
| УБИ.051 | Уг­ро­за не­воз­можнос­ти вос­ста­нов­ле­ния сес­сии ра­боты на ПЭВМ при вы­воде из про­межу­точ­ных сос­то­яний пи­тания |
| УБИ.053 | Уг­ро­за не­воз­можнос­ти уп­равле­ния пра­вами поль­зо­вате­лей BIOS |
| УБИ.058 | Уг­ро­за не­кон­тро­лиру­емо­го рос­та чис­ла вир­ту­аль­ных ма­шин |
| УБИ.059 | Уг­ро­за не­кон­тро­лиру­емо­го рос­та чис­ла за­резер­ви­рован­ных вы­чис­ли­тель­ных ре­сур­сов |
| УБИ.061 | Уг­ро­за не­кор­рек­тно­го за­дания струк­ту­ры дан­ных тран­закции |
| УБИ.062 | Уг­ро­за не­кор­рек­тно­го ис­поль­зо­вания проз­рачно­го прок­си-сер­ве­ра за счёт пла­гинов бра­узе­ра |
| УБИ.063 | Уг­ро­за не­кор­рек­тно­го ис­поль­зо­вания фун­кци­она­ла прог­рам­мно­го и ап­па­рат­но­го обес­пе­чения |
| УБИ.064 | Уг­ро­за не­кор­рек­тной ре­али­зации по­лити­ки ли­цен­зи­рова­ния в об­ла­ке |
| УБИ.067 | Уг­ро­за неп­ра­вомер­но­го оз­на­ком­ле­ния с за­щища­емой ин­форма­цией |
| УБИ.068 | Уг­ро­за неп­ра­вомер­но­го/не­кор­рек­тно­го ис­поль­зо­вания ин­терфей­са вза­имо­дей­ствия с при­ложе­ни­ем |
| УБИ.069 | Уг­ро­за неп­ра­вомер­ных дей­ствий в ка­налах свя­зи |
| УБИ.071 | Уг­ро­за не­сан­кци­они­рован­но­го вос­ста­нов­ле­ния уда­лён­ной за­щища­емой ин­форма­ции |
| УБИ.072 | Уг­ро­за не­сан­кци­они­рован­но­го вык­лю­чения или об­хо­да ме­ханиз­ма за­щиты от за­писи в BIOS |
| УБИ.073 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к ак­тивно­му и (или) пас­сивно­му вир­ту­аль­но­му и (или) фи­зичес­ко­му се­тево­му обо­рудо­ванию из фи­зичес­кой и (или) вир­ту­аль­ной се­ти |
| УБИ.074 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к а­утен­ти­фика­ци­он­ной ин­форма­ции |
| УБИ.075 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к вир­ту­аль­ным ка­налам пе­реда­чи |
| УБИ.076 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к ги­пер­ви­зору из вир­ту­аль­ной ма­шины и (или) фи­зичес­кой се­ти |
| УБИ.077 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к дан­ным за пре­дела­ми за­резер­ви­рован­но­го ад­ресно­го прос­транс­тва, в том чис­ле вы­делен­но­го под вир­ту­аль­ное ап­па­рат­ное обес­пе­чение |
| УБИ.078 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емым вир­ту­аль­ным ма­шинам из вир­ту­аль­ной и (или) фи­зичес­кой се­ти |
| УБИ.079 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емым вир­ту­аль­ным ма­шинам со сто­роны дру­гих вир­ту­аль­ных ма­шин |
| УБИ.080 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емым вир­ту­аль­ным ус­трой­ствам из вир­ту­аль­ной и (или) фи­зичес­кой се­ти |
| УБИ.084 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к сис­те­ме хра­нения дан­ных из вир­ту­аль­ной и (или) фи­зичес­кой се­ти |
| УБИ.085 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к хра­нимой в вир­ту­аль­ном прос­транс­тве за­щища­емой ин­форма­ции |
| УБИ.086 | Уг­ро­за не­сан­кци­они­рован­но­го из­ме­нения а­утен­ти­фика­ци­он­ной ин­форма­ции |
| УБИ.087 | Уг­ро­за не­сан­кци­они­рован­но­го ис­поль­зо­вания при­виле­гиро­ван­ных фун­кций BIOS |
| УБИ.088 | Уг­ро­за не­сан­кци­они­рован­но­го ко­пиро­вания за­щища­емой ин­форма­ции |
| УБИ.089 | Уг­ро­за не­сан­кци­они­рован­но­го ре­дак­ти­рова­ния ре­ес­тра |
| УБИ.090 | Уг­ро­за не­сан­кци­они­рован­но­го соз­да­ния учёт­ной за­писи поль­зо­вате­ля |
| УБИ.091 | Уг­ро­за не­сан­кци­они­рован­но­го уда­ления за­щища­емой ин­форма­ции |
| УБИ.093 | Уг­ро­за не­сан­кци­они­рован­но­го уп­равле­ния бу­фером |
| УБИ.094 | Уг­ро­за не­сан­кци­они­рован­но­го уп­равле­ния син­хро­низа­цией и сос­то­яни­ем |
| УБИ.095 | Уг­ро­за не­сан­кци­они­рован­но­го уп­равле­ния ука­зате­лями |
| УБИ.098 | Уг­ро­за об­на­руже­ния от­кры­тых пор­тов и иден­ти­фика­ции при­вязан­ных к ним се­тевых служб |
| УБИ.099 | Уг­ро­за об­на­руже­ния хос­тов |
| УБИ.100 | Уг­ро­за об­хо­да не­кор­рек­тно нас­тро­ен­ных ме­ханиз­мов а­утен­ти­фика­ции |
| УБИ.102 | Уг­ро­за опос­ре­дован­но­го уп­равле­ния груп­пой прог­рамм че­рез сов­мес­тно ис­поль­зу­емые дан­ные |
| УБИ.103 | Уг­ро­за оп­ре­деле­ния ти­пов объ­ек­тов за­щиты |
| УБИ.104 | Уг­ро­за оп­ре­деле­ния то­поло­гии вы­чис­ли­тель­ной се­ти |
| УБИ.108 | Уг­ро­за ошиб­ки об­новле­ния ги­пер­ви­зора |
| УБИ.109 | Уг­ро­за пе­ребо­ра всех нас­тро­ек и па­рамет­ров при­ложе­ния |
| УБИ.111 | Уг­ро­за пе­реда­чи дан­ных по скры­тым ка­налам |
| УБИ.113 | Уг­ро­за пе­резаг­рузки ап­па­рат­ных и прог­рам­мно-ап­па­рат­ных средств вы­чис­ли­тель­ной тех­ни­ки |
| УБИ.114 | Уг­ро­за пе­репол­не­ния це­лочис­ленных пе­ремен­ных |
| УБИ.115 | Уг­ро­за пе­рех­ва­та вво­димой и вы­води­мой на пе­рифе­рий­ные ус­трой­ства ин­форма­ции |
| УБИ.116 | Уг­ро­за пе­рех­ва­та дан­ных, пе­реда­ва­емых по вы­чис­ли­тель­ной се­ти |
| УБИ.117 | Уг­ро­за пе­рех­ва­та при­виле­гиро­ван­но­го по­тока |
| УБИ.118 | Уг­ро­за пе­рех­ва­та при­виле­гиро­ван­но­го про­цес­са |
| УБИ.119 | Уг­ро­за пе­рех­ва­та уп­равле­ния ги­пер­ви­зором |
| УБИ.120 | Уг­ро­за пе­рех­ва­та уп­равле­ния сре­дой вир­ту­али­зации |
| УБИ.121 | Уг­ро­за пов­режде­ния сис­темно­го ре­ес­тра |
| УБИ.122 | Уг­ро­за по­выше­ния при­виле­гий |
| УБИ.123 | Уг­ро­за под­бо­ра па­роля BIOS |
| УБИ.124 | Уг­ро­за под­делки за­писей жур­на­ла ре­гис­тра­ции со­бытий |
| УБИ.127 | Уг­ро­за под­ме­ны дей­ствия поль­зо­вате­ля пу­тём об­ма­на |
| УБИ.128 | Уг­ро­за под­ме­ны до­верен­но­го поль­зо­вате­ля |
| УБИ.129 | Уг­ро­за под­ме­ны ре­зер­вной ко­пии прог­рам­мно­го обес­пе­чения BIOS |
| УБИ.130 | Уг­ро­за под­ме­ны со­дер­жи­мого се­тевых ре­сур­сов |
| УБИ.131 | Уг­ро­за под­ме­ны субъ­ек­та се­тево­го дос­ту­па |
| УБИ.132 | Уг­ро­за по­луче­ния пред­ва­ритель­ной ин­форма­ции об объ­ек­те за­щиты |
| УБИ.139 | Уг­ро­за пре­одо­ления фи­зичес­кой за­щиты |
| УБИ.140 | Уг­ро­за при­веде­ния сис­те­мы в сос­то­яние «от­каз в об­слу­жива­нии» |
| УБИ.143 | Уг­ро­за прог­рам­мно­го вы­веде­ния из строя средств хра­нения, об­ра­бот­ки и (или) вво­да/вы­вода/пе­реда­чи ин­форма­ции |
| УБИ.144 | Уг­ро­за прог­рам­мно­го сбро­са па­роля BIOS |
| УБИ.145 | Уг­ро­за про­пус­ка про­вер­ки це­лос­тнос­ти прог­рам­мно­го обес­пе­чения |
| УБИ.149 | Уг­ро­за сбоя об­ра­бот­ки спе­ци­аль­ным об­ра­зом из­ме­нён­ных фай­лов |
| УБИ.150 | Уг­ро­за сбоя про­цес­са об­новле­ния BIOS |
| УБИ.151 | Уг­ро­за ска­ниро­вания веб-сер­ви­сов, раз­ра­ботан­ных на ос­но­ве язы­ка опи­сания WSDL |
| УБИ.152 | Уг­ро­за уда­ления а­утен­ти­фика­ци­он­ной ин­форма­ции |
| УБИ.153 | Уг­ро­за уси­ления воз­дей­ствия на вы­чис­ли­тель­ные ре­сур­сы поль­зо­вате­лей при по­мощи сто­рон­них сер­ве­ров |
| УБИ.154 | Уг­ро­за ус­та­нов­ки у­яз­ви­мых вер­сий об­новле­ния прог­рам­мно­го обес­пе­чения BIOS |
| УБИ.155 | Уг­ро­за ут­ра­ты вы­чис­ли­тель­ных ре­сур­сов |
| УБИ.156 | Уг­ро­за ут­ра­ты но­сите­лей ин­форма­ции |
| УБИ.157 | Уг­ро­за фи­зичес­ко­го вы­веде­ния из строя средств хра­нения, об­ра­бот­ки и (или) вво­да/вы­вода/пе­реда­чи ин­форма­ции |
| УБИ.158 | Уг­ро­за фор­ма­тиро­вания но­сите­лей ин­форма­ции |
| УБИ.159 | Уг­ро­за «фор­си­рован­но­го веб-бра­узин­га» |
| УБИ.160 | Уг­ро­за хи­щения средств хра­нения, об­ра­бот­ки и (или) вво­да/вы­вода/пе­реда­чи ин­форма­ции |
| УБИ.162 | Уг­ро­за экс­плу­ата­ции циф­ро­вой под­пи­си прог­рам­мно­го ко­да |
| УБИ.163 | Уг­ро­за пе­рех­ва­та ис­клю­чения/сиг­на­ла из при­виле­гиро­ван­но­го бло­ка фун­кций |
| УБИ.165 | Уг­ро­за вклю­чения в про­ект не дос­то­вер­но ис­пы­тан­ных ком­по­нен­тов |
| УБИ.166 | Уг­ро­за внед­ре­ния сис­темной из­бы­точ­ности |
| УБИ.167 | Уг­ро­за за­раже­ния компь­юте­ра при по­сеще­нии неб­ла­гона­дёж­ных сай­тов |
| УБИ.168 | Уг­ро­за «кра­жи» учёт­ной за­писи дос­ту­па к се­тевым сер­ви­сам |
| УБИ.169 | Уг­ро­за на­личия ме­ханиз­мов раз­ра­бот­чи­ка |
| УБИ.170 | Уг­ро­за неп­ра­вомер­но­го шиф­ро­вания ин­форма­ции |
| УБИ.171 | Уг­ро­за скрыт­но­го вклю­чения вы­чис­ли­тель­но­го ус­трой­ства в сос­тав бот-се­ти |
| УБИ.172 | Уг­ро­за рас­простра­нения «поч­то­вых чер­вей» |
| УБИ.173 | Уг­ро­за «спа­ма» веб-сер­ве­ра |
| УБИ.174 | Уг­ро­за «фар­минга» |
| УБИ.175 | Уг­ро­за «фи­шин­га» |
| УБИ.176 | Уг­ро­за на­руше­ния тех­но­логи­чес­ко­го/про­из­водс­твен­но­го про­цес­са из-за вре­мен­ны́х за­дер­жек, вно­симых средс­твом за­щиты |
| УБИ.177 | Уг­ро­за не­под­тверждён­но­го вво­да дан­ных опе­рато­ром в сис­те­му, свя­зан­ную с бе­зопас­ностью |
| УБИ.178 | Уг­ро­за не­сан­кци­они­рован­но­го ис­поль­зо­вания сис­темных и се­тевых ути­лит |
| УБИ.179 | Уг­ро­за не­сан­кци­они­рован­ной мо­дифи­кации за­щища­емой ин­форма­ции |
| УБИ.180 | Уг­ро­за от­ка­за под­систе­мы обес­пе­чения тем­пе­ратур­но­го ре­жима |
| УБИ.182 | Уг­ро­за фи­зичес­ко­го ус­та­рева­ния ап­па­рат­ных ком­по­нен­тов |
| УБИ.185 | Уг­ро­за не­сан­кци­они­рован­но­го из­ме­нения па­рамет­ров нас­трой­ки средств за­щиты ин­форма­ции |
| УБИ.186 | Уг­ро­за внед­ре­ния вре­донос­но­го ко­да че­рез рек­ла­му, сер­ви­сы и кон­тент |
| УБИ.187 | Уг­ро­за не­сан­кци­они­рован­но­го воз­дей­ствия на средс­тво за­щиты ин­форма­ции |
| УБИ.188 | Уг­ро­за под­ме­ны прог­рам­мно­го обес­пе­чения |
| УБИ.189 | Уг­ро­за мас­ки­рова­ния дей­ствий вре­донос­но­го ко­да |
| УБИ.190 | Уг­ро­за внед­ре­ния вре­донос­но­го ко­да за счет по­сеще­ния за­ражен­ных сай­тов в се­ти Ин­тернет |
| УБИ.191 | Уг­ро­за внед­ре­ния вре­донос­но­го ко­да в дис­три­бутив прог­рам­мно­го обес­пе­чения |
| УБИ.192 | Уг­ро­за ис­поль­зо­вания у­яз­ви­мых вер­сий прог­рам­мно­го обес­пе­чения |
| УБИ.198 | Уг­ро­за скрыт­ной ре­гис­тра­ции вре­донос­ной прог­раммой учет­ных за­писей ад­ми­нис­тра­торов |
| УБИ.203 | Уг­ро­за утеч­ки ин­форма­ции с не­под­клю­чен­ных к се­ти Ин­тернет компь­юте­ров |
| УБИ.205 | Уг­ро­за на­руше­ния ра­боты компь­юте­ра и бло­киро­вания дос­ту­па к его дан­ным из-за не­кор­рек­тной ра­боты ус­та­нов­ленных на нем средств за­щиты |
| УБИ.208 | Уг­ро­за не­целе­вого ис­поль­зо­вания вы­чис­ли­тель­ных ре­сур­сов средс­тва вы­чис­ли­тель­ной тех­ни­ки |
| УБИ.209 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емой па­мяти яд­ра про­цес­со­ра |
| УБИ.211 | Уг­ро­за ис­поль­зо­вания неп­ро­верен­ных поль­зо­ватель­ских дан­ных при фор­ми­рова­нии кон­фи­гура­ци­он­но­го фай­ла, ис­поль­зу­емо­го прог­рам­мным обес­пе­чени­ем ад­ми­нис­три­рова­ния ин­форма­ци­он­ных сис­тем |
| УБИ.212 | Уг­ро­за пе­рех­ва­та уп­равле­ния ин­форма­ци­он­ной сис­те­мой |
| УБИ.214 | Уг­ро­за нес­во­ев­ре­мен­но­го вы­яв­ле­ния и ре­аги­рова­ния ком­по­нен­та­ми ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мы (в том чис­ле средс­тва­ми за­щиты ин­форма­ции) на со­бытия бе­зопас­ности ин­форма­ции |
| УБИ.215 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к сис­те­ме при по­мощи сто­рон­них сер­ви­сов |
| УБИ.217 | Уг­ро­за ис­поль­зо­вания ском­про­мети­рован­но­го до­верен­но­го ис­точни­ка об­новле­ний прог­рам­мно­го обес­пе­чения |

1. Оценка угроз в соответствии с методическими документами ФСБ России
   1. На основании исходных данных об объектах защиты (в соответствии с разделом 5 настоящей Модели угроз) и источниках атак (в соответствии с разделом 6.1 настоящей Модели угроз) ГИС в сфере финансов определены обобщенные возможности источников атак (таблица 17).

Таблица 17 – Обобщенные возможности источников атак

| № | Обоб­щен­ные воз­мож­ности ис­точ­ников атак | Пред­поло­же­ние  о возможности источников атак |
| --- | --- | --- |
| 1. | Воз­можность са­мос­то­ятель­но осу­щест­влять соз­да­ние спо­собов атак, под­го­тов­ку и про­веде­ние атак толь­ко за пре­дела­ми кон­тро­лиру­емой зо­ны | Да |
| 2. | Воз­можность са­мос­то­ятель­но осу­щест­влять соз­да­ние спо­собов атак, под­го­тов­ку и про­веде­ние атак в пре­делах кон­тро­лиру­емой зо­ны, но без фи­зичес­ко­го дос­ту­па к ап­па­рат­ным средс­твам, на ко­торых ре­али­зова­ны СКЗИ и сре­да их фун­кци­они­рова­ния | Да |
| 3. | Воз­можность са­мос­то­ятель­но осу­щест­влять соз­да­ние спо­собов атак, под­го­тов­ку и про­веде­ние атак в пре­делах кон­тро­лиру­емой зо­ны с фи­зичес­ким дос­ту­пом к ап­па­рат­ным средс­твам, на ко­торых ре­али­зова­ны СКЗИ и сре­да их фун­кци­они­рова­ния | Нет |
| 4. | Воз­можность прив­ле­кать спе­ци­алис­тов, име­ющих опыт раз­ра­бот­ки и ана­лиза СКЗИ (вклю­чая спе­ци­алис­тов в об­ласти ана­лиза сиг­на­лов ли­ней­ной пе­реда­чи и сиг­на­лов по­боч­но­го элек­тро­маг­нитно­го из­лу­чения и на­водок СКЗИ) | Нет |
| 5. | Воз­можность прив­ле­кать спе­ци­алис­тов, име­ющих опыт раз­ра­бот­ки и ана­лиза СКЗИ (вклю­чая спе­ци­алис­тов в об­ласти ис­поль­зо­вания для ре­али­зации атак не­доку­мен­ти­рован­ных воз­можнос­тей прик­ладно­го прог­рам­мно­го обес­пе­чения) | Нет |
| 6. | Воз­можность прив­ле­кать спе­ци­алис­тов, име­ющих опыт раз­ра­бот­ки и ана­лиза СКЗИ (вклю­чая спе­ци­алис­тов в об­ласти ис­поль­зо­вания для ре­али­зации атак не­доку­мен­ти­рован­ных воз­можнос­тей ап­па­рат­но­го и прог­рам­мно­го ком­по­нен­тов сре­ды фун­кци­они­рова­ния СКЗИ) | Нет |

* 1. В соответствии с нормативно-правовыми документами ФСБ России реализация угроз безопасности информации определяется возможностями источников атак.
  2. Исходя из обобщенных возможностей источников атак определены уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы). Результаты приведены в Приложении № 7.
  3. Используемые для защиты информации криптосредства должны обеспечить криптографическую защиту по уровню не ниже КС2.

Приложение № 1

Источники разработки модели угроз

Система должна соответствовать требованиям следующих Федеральных законов и принятых в соответствии с ними нормативно-правовых актов:

* Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
* Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
* Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Методический документ «Методика оценки угроз безопасности информации», утвержденный Федеральной службы по техническому и экспортному контролю 5 февраля 2021 г.;
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г.;
* Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра Федеральной службы безопасности Российской Федерации 31 марта 2015 г. № 149/7/2/6-432;
* 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 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 457-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** | **Вид 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. | Тер­ро­рис­ти­чес­кие, экс­тре­мист­ские груп­пи­ров­ки | Со­вер­ше­ние тер­ро­рис­ти­чес­ких ак­тов, уг­ро­за жиз­ни граж­дан | НП.3 | НП.8; НП.13; НП.15; НП.16 | НП.23 |
| На­несе­ние ущер­ба от­дель­ным сфе­рам де­ятель­нос­ти или сек­то­рам эко­номи­ки го­сударс­тва | – | – | НП.22; НП.23 |
| Дес­та­били­зация об­щес­тва | – | – | – |
| Дес­та­били­зация де­ятель­нос­ти ор­га­нов го­сударс­твен­ной влас­ти, ор­га­низа­ций | – | – | НП.2; НП.21; НП.24 |
| 2. | Прес­тупные груп­пы (кри­миналь­ные струк­ту­ры) | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | – | НП.9 | – |
| Же­лание са­море­али­зации (под­твержде­ние ста­туса) | НП.1; НП.7 | НП.12; НП.13; НП.14; НП.15; НП.16; НП.19 | – |
| 3. | От­дель­ные фи­зичес­кие ли­ца (ха­керы) | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | – |
| Лю­бопытс­тво или же­лание са­море­али­зации (под­твержде­ние ста­туса) | НП.1; НП.7 | НП.12; НП.13; НП.14; НП.15; НП.16; НП.19 | – |
| 4. | Кон­ку­риру­ющие ор­га­низа­ции | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | – | НП.9 | – |
| По­луче­ние кон­ку­рен­тных пре­иму­ществ | – | НП.10; НП.14; НП.19 | – |
| 5. | Раз­ра­бот­чи­ки прог­рам­мных, прог­рам­мно-ап­па­рат­ных средств | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | НП.22; НП.23 |
| По­луче­ние кон­ку­рен­тных пре­иму­ществ | – | НП.10; НП.14; НП.19 | – |
| Внед­ре­ние до­пол­ни­тель­ных фун­кци­ональ­ных воз­можнос­тей в прог­рам­мные или прог­рам­мно-ап­па­рат­ные средс­тва на эта­пе раз­ра­бот­ки | НП.1; НП.5; НП.7 | НП.12; НП.19 | НП.20 |
| Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия | НП.1; НП.7 | НП.12; НП.13; НП.15; НП.16; НП.17; НП.19 | НП.20; НП.21 |
| 6. | Ли­ца, обес­пе­чива­ющие пос­тавку прог­рам­мных, прог­рам­мно-ап­па­рат­ных средств, обес­пе­чива­ющих сис­тем | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | – |
| По­луче­ние кон­ку­рен­тных пре­иму­ществ | НП.7 | – | – |
| Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия | НП.1; НП.7 | НП.8; НП.11; НП.12; НП.13 | – |
| 7. | Пос­тавщи­ки вы­чис­ли­тель­ных ус­луг, ус­луг свя­зи | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | – |
| По­луче­ние кон­ку­рен­тных пре­иму­ществ | – | НП.19 | – |
| Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия | НП.1; НП.7 | НП.8; НП.11; НП.12; НП.13; НП.14; НП.15; НП.19 | – |
| 8. | Ли­ца, прив­ле­ка­емые для ус­та­нов­ки, нас­трой­ки, ис­пы­таний, пус­ко­нала­доч­ных и иных ви­дов ра­бот | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9; НП.17 | – |
| По­луче­ние кон­ку­рен­тных пре­иму­ществ | – | НП.19 | – |
| Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия | НП.1; НП.7 | НП.8; НП.11; НП.12; НП.13; НП.14; НП.15; НП.19 | – |
| 9. | Ли­ца, обес­пе­чива­ющие фун­кци­они­рова­ние сис­тем и се­тей или обес­пе­чива­ющие сис­те­мы опе­рато­ра | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | – |
| Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия | НП.1; НП.7 | НП.8; НП.11; НП.12; НП.13; НП.19 | – |
| 10. | Ав­то­ризо­ван­ные поль­зо­вате­ли сис­тем и се­тей | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | НП.23 |
| Лю­бопытс­тво или же­лание са­море­али­зации (под­твержде­ние ста­туса) | НП.1; НП.5; НП.7 | НП.14; НП.19 | – |
| Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия | НП.1; НП.5; НП.7 | НП.8; НП.11; НП.12; НП.13; НП.17; НП.19 | НП.20 |
| Месть за ра­нее со­вер­шенные дей­ствия | НП.1; НП.4; НП.5; НП.7 | – | – |
| 11. | Сис­темные ад­ми­нис­тра­торы и ад­ми­нис­тра­торы бе­зопас­ности | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | НП.23 |
| Лю­бопытс­тво или же­лание са­море­али­зации (под­твержде­ние ста­туса) | НП.1; НП.7 | НП.14; НП.19 | – |
| Неп­редна­мерен­ные, не­ос­то­рож­ные или нек­ва­лифи­циро­ван­ные дей­ствия | НП.1; НП.5; НП.7 | НП.8; НП.11; НП.12; НП.13; НП.15; НП.17; НП.18; НП.19 | НП.2; НП.20; НП.21; НП.24 |
| Месть за ра­нее со­вер­шенные дей­ствия | НП.1; НП.4; НП.5; НП.7 | НП.14 | – |
| 12. | Быв­шие (уво­лен­ные) ра­бот­ни­ки (поль­зо­вате­ли) | По­луче­ние фи­нан­со­вой или иной ма­тери­аль­ной вы­годы | НП.7 | НП.9 | НП.23 |
| Месть за ра­нее со­вер­шенные дей­ствия | НП.1; НП.4; НП.5; НП.7 | НП.14 | – |

Приложение № 3

Уровни возможностей нарушителя

| **№** | **Уровень воз­мож­нос­тей на­ру­ши­те­лей** | **Возможности нарушителей по реализации угроз безопасности** |
| --- | --- | --- |
| 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, 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 из базового перечня угроз безопасности информации

| **Иден­ти­фи­ка­тор уг­ро­зы** | **Наи­ме­но­вание угрозы** | **Обоснование исключения из числа возможных угроз безопасности информации** |
| --- | --- | --- |
| УБИ.001 | Уг­ро­за ав­то­мати­чес­ко­го рас­простра­нения вре­донос­но­го ко­да в грид-сис­те­ме | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.002 | Уг­ро­за аг­ре­гиро­вания дан­ных, пе­реда­ва­емых в грид-сис­те­ме | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.005 | Уг­ро­за внед­ре­ния вре­донос­но­го ко­да в BIOS | Уро­вень воз­можнос­тей на­руши­телей не­дос­та­точен для ре­али­зации уг­ро­зы |
| УБИ.011 | Уг­ро­за де­ав­то­риза­ции сан­кци­они­рован­но­го кли­ен­та бес­про­вод­ной се­ти | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.017 | Уг­ро­за дос­ту­па/пе­рех­ва­та/из­ме­нения HTTP cookies | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.020 | Уг­ро­за зло­упот­ребле­ния воз­можнос­тя­ми, пре­дос­тавлен­ны­ми пот­ре­бите­лям об­лачных ус­луг | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.021 | Уг­ро­за зло­упот­ребле­ния до­вери­ем пот­ре­бите­лей об­лачных ус­луг | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.024 | Уг­ро­за из­ме­нения ре­жимов ра­боты ап­па­рат­ных эле­мен­тов компь­юте­ра | Уро­вень воз­можнос­тей на­руши­телей не­дос­та­точен для ре­али­зации уг­ро­зы |
| УБИ.026 | Уг­ро­за ис­ка­жения XML-схе­мы | 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.029 | Уг­ро­за ис­поль­зо­вания вы­чис­ли­тель­ных ре­сур­сов су­пер­компь­юте­ра «па­разит­ны­ми» про­цес­са­ми | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.035 | Уг­ро­за ис­поль­зо­вания сла­бых крип­тогра­фичес­ких ал­го­рит­мов BIOS | Уро­вень воз­можнос­тей на­руши­телей не­дос­та­точен для ре­али­зации уг­ро­зы |
| УБИ.038 | Уг­ро­за ис­черпа­ния вы­чис­ли­тель­ных ре­сур­сов хра­нили­ща боль­ших дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.040 | Уг­ро­за кон­флик­та юрис­дикций раз­личных стран | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.043 | Уг­ро­за на­руше­ния дос­тупнос­ти об­лачно­го сер­ве­ра | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.047 | Уг­ро­за на­руше­ния ра­ботос­по­соб­ности грид-сис­те­мы при не­типич­ной се­тевой наг­рузке | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.050 | Уг­ро­за не­вер­но­го оп­ре­деле­ния фор­ма­та вход­ных дан­ных, пос­ту­па­ющих в хра­нили­ще боль­ших дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.052 | Уг­ро­за не­воз­можнос­ти миг­ра­ции об­ра­зов вир­ту­аль­ных ма­шин из-за не­сов­мести­мос­ти ап­па­рат­но­го и прог­рам­мно­го обес­пе­чения | 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.054 | Уг­ро­за не­доб­ро­совес­тно­го ис­полне­ния обя­затель­ств пос­тавщи­ками об­лачных ус­луг | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.055 | Уг­ро­за не­защи­щён­но­го ад­ми­нис­три­рова­ния об­лачных ус­луг | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.056 | Уг­ро­за не­качес­твен­но­го пе­рено­са ин­фраструк­ту­ры в об­ла­ко | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.057 | Уг­ро­за не­кон­тро­лиру­емо­го ко­пиро­вания дан­ных внут­ри хра­нили­ща боль­ших дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.060 | Уг­ро­за не­кон­тро­лиру­емо­го унич­то­жения ин­форма­ции хра­нили­щем боль­ших дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.065 | Уг­ро­за не­оп­ре­делён­ности в рас­пре­деле­нии от­ветс­твен­ности меж­ду ро­лями в об­ла­ке | 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.066 | Уг­ро­за не­оп­ре­делён­ности от­ветс­твен­ности за обес­пе­чение бе­зопас­ности об­ла­ка | 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.070 | Уг­ро­за неп­ре­рыв­ной мо­дер­ни­зации об­лачной ин­фраструк­ту­ры | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.081 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к ло­каль­но­му компь­юте­ру че­рез кли­ен­та грид-сис­те­мы | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.082 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к сег­ментам вы­чис­ли­тель­но­го по­ля | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.083 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к сис­те­ме по бес­про­вод­ным ка­налам | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.092 | Уг­ро­за не­сан­кци­они­рован­но­го уда­лён­но­го вне­полос­но­го дос­ту­па к ап­па­рат­ным средс­твам | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.096 | Уг­ро­за не­сог­ла­сован­ности по­литик бе­зопас­ности эле­мен­тов об­лачной ин­фраструк­ту­ры | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.097 | Уг­ро­за не­сог­ла­сован­ности пра­вил дос­ту­па к боль­шим дан­ным | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.101 | Уг­ро­за об­ще­дос­тупнос­ти об­лачной ин­фраструк­ту­ры | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.105 | Уг­ро­за от­ка­за в заг­рузке вход­ных дан­ных не­из­вес­тно­го фор­ма­та хра­нили­щем боль­ших дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.106 | Уг­ро­за от­ка­за в об­слу­жива­нии сис­те­мой хра­нения дан­ных су­пер­компь­юте­ра | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.107 | Уг­ро­за от­клю­чения кон­троль­ных дат­чи­ков | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.110 | Уг­ро­за пе­рег­рузки грид-сис­те­мы вы­чис­ли­тель­ны­ми за­дани­ями | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.112 | Уг­ро­за пе­реда­чи зап­ре­щён­ных ко­манд на обо­рудо­вание с чис­ло­вым прог­рам­мным уп­равле­ни­ем | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.125 | Уг­ро­за под­клю­чения к бес­про­вод­ной се­ти в об­ход про­цеду­ры а­утен­ти­фика­ции | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.126 | Уг­ро­за под­ме­ны бес­про­вод­но­го кли­ен­та или точ­ки дос­ту­па | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.133 | Уг­ро­за по­луче­ния све­дений о вла­дель­це бес­про­вод­но­го ус­трой­ства | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.134 | Уг­ро­за по­тери до­верия к пос­тавщи­ку об­лачных ус­луг | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.135 | Уг­ро­за по­тери и утеч­ки дан­ных, об­ра­баты­ва­емых в об­ла­ке | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.136 | Уг­ро­за по­тери ин­форма­ции вследс­твие не­сог­ла­сован­ности ра­боты уз­лов хра­нили­ща боль­ших дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.137 | Уг­ро­за по­тери уп­равле­ния об­лачны­ми ре­сур­са­ми | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.138 | Уг­ро­за по­тери уп­равле­ния собс­твен­ной ин­фраструк­ту­рой при пе­рено­се её в об­ла­ко | 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 | Уг­ро­за при­вяз­ки к пос­тавщи­ку об­лачных ус­луг | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.142 | Уг­ро­за при­ос­та­нов­ки ока­зания об­лачных ус­луг вследс­твие тех­ни­чес­ких сбо­ев | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.146 | Уг­ро­за пря­мого об­ра­щения к па­мяти вы­чис­ли­тель­но­го по­ля су­пер­компь­юте­ра | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.147 | Уг­ро­за рас­простра­нения не­сан­кци­они­рован­но по­вышен­ных прав на всю грид-сис­те­му | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.148 | Уг­ро­за сбоя ав­то­мати­чес­ко­го уп­равле­ния сис­те­мой раз­гра­ниче­ния дос­ту­па хра­нили­ща боль­ших дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.161 | Уг­ро­за чрез­мерно­го ис­поль­зо­вания вы­чис­ли­тель­ных ре­сур­сов су­пер­компь­юте­ра в хо­де ин­тенсив­но­го об­ме­на меж­про­цес­сорны­ми со­об­ще­ни­ями | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.164 | Уг­ро­за рас­простра­нения сос­то­яния «от­каз в об­слу­жива­нии» в об­лачной ин­фраструк­ту­ре | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.181 | Уг­ро­за пе­рех­ва­та од­но­разо­вых па­ролей в ре­жиме ре­аль­но­го вре­мени | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.183 | Уг­ро­за пе­рех­ва­та уп­равле­ния ав­то­мати­зиро­ван­ной сис­те­мой уп­равле­ния тех­но­логи­чес­ки­ми про­цес­са­ми | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.184 | Уг­ро­за аг­ре­гиро­вания дан­ных, об­ра­баты­ва­емых с по­мощью мо­биль­но­го ус­трой­ства | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| 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 на­руши­телей не­дос­та­точен для ре­али­зации уг­ро­зы |
| УБИ.196 | Уг­ро­за кон­тро­ля вре­донос­ной прог­раммой спис­ка при­ложе­ний, за­пущен­ных на мо­биль­ном ус­трой­стве | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.197 | Уг­ро­за хи­щения а­утен­ти­фика­ци­он­ной ин­форма­ции из вре­мен­ных фай­лов cookie | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.199 | Уг­ро­за пе­рех­ва­та уп­равле­ния мо­биль­но­го ус­трой­ства при ис­поль­зо­вании вир­ту­аль­ных го­лосо­вых ас­систен­тов | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.200 | Уг­ро­за хи­щения ин­форма­ции с мо­биль­но­го ус­трой­ства при ис­поль­зо­вании вир­ту­аль­ных го­лосо­вых ас­систен­тов | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| 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 | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.206 | Уг­ро­за от­ка­за в ра­боте обо­рудо­вания из-за из­ме­нения ге­оло­каци­он­ной ин­форма­ции о нем | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.207 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к па­рамет­рам нас­трой­ки обо­рудо­вания за счет ис­поль­зо­вания «мас­тер-ко­дов» (ин­же­нер­ных па­ролей) | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.210 | Уг­ро­за на­руше­ния ра­боты ин­форма­ци­он­ной сис­те­мы, выз­ванно­го об­новле­ни­ем ис­поль­зу­емо­го в ней прог­рам­мно­го обес­пе­чения | Уро­вень воз­можнос­тей на­руши­телей не­дос­та­точен для ре­али­зации уг­ро­зы |
| УБИ.213 | Уг­ро­за об­хо­да мно­гофак­торной а­утен­ти­фика­ции | Уро­вень воз­можнос­тей на­руши­телей не­дос­та­точен для ре­али­зации уг­ро­зы |
| УБИ.216 | Уг­ро­за по­луче­ния не­сан­кци­они­рован­но­го дос­ту­па к при­ложе­ни­ям, ус­та­нов­ленным на Smart-кар­тах | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.218 | Уг­ро­за рас­кры­тия ин­форма­ции о мо­дели ма­шин­но­го обу­чения | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.219 | Уг­ро­за хи­щения обу­ча­ющих дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.220 | Уг­ро­за на­руше­ния фун­кци­они­рова­ния («об­хо­да») средств, ре­али­зу­ющих тех­но­логии ис­кусс­твен­но­го ин­теллек­та | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.221 | Уг­ро­за мо­дифи­кации мо­дели ма­шин­но­го обу­чения пу­тем ис­ка­жения («от­равле­ния») обу­ча­ющих дан­ных | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |
| УБИ.222 | Уг­ро­за под­ме­ны мо­дели ма­шин­но­го обу­чения | От­сутс­тву­ют объ­ек­ты воз­дей­ствия |

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 | T1.1 Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций |
| T1.2 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 |
| T1.3 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 |
| T1.4 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 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 |
| T1.21 Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем анализа и обобщения информации перехватываемой в сети передачи информации |
| T1.22 Поиск и покупка специализированного программного обеспечения (вредоносного кода) на специализированных нелегальных площадках |
| 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 |
| 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) |
| 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 |
| Т2.15 Доступ путем использования недостатков правовых норм других стран, участвующих в трансграничной передаче облачного трафика |
| Т2.16 Доступ путем использования возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако |
| 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. «дарквеб») 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 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 |
| T3.17 Планирование запуска вредоносного кода при запуске компьютера путем эксплуатации стандартных механизмов BIOS (UEFI) и т.п. |
| T3.18 Эксплуатация уязвимостей типа локальное исполнение программного кода |
| 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 |
| T4.8 Использование прошивок устройств с уязвимостями, к примеру, внедрение новых функций в BIOS (UEFI) |
| 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 |
| 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. |
| T5.13 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 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 |
| 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 |
| 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 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** |
| --- | --- | --- | --- | --- | --- | --- |
| УБИ.003 | Уг­ро­за ис­поль­зо­вания сла­бос­тей крип­тогра­фичес­ких ал­го­рит­мов и у­яз­ви­мос­тей в прог­рам­мном обес­пе­чении их ре­али­зации | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тва крип­тогра­фичес­кой за­щиты ин­форма­ции | НП.7; НП.12; НП.15; НП.16; НП.20 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.003:   * Т1 (Т1.9; Т1.16); * Т2 (Т2.5); * Т10 (Т10.2; Т10.5) |
| УБИ.004 | Уг­ро­за ап­па­рат­но­го сбро­са па­роля BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.9; СР.11 | Сце­нарий ре­али­зации УБИ.004:   * Т1 (Т1.9; Т1.15; Т1.16); * Т2 (Т2.9) |
| УБИ.006 | Уг­ро­за внед­ре­ния ко­да или дан­ных | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.2; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.006:   * Т1 (T1.4; Т1.5); * Т2 (Т2.5; Т2.10); * Т3 (Т3.1; Т3.2; Т3.15); * Т4 (Т4.2); * Т5 (Т5.2) |
| УБИ.007 | Уг­ро­за воз­дей­ствия на прог­раммы с вы­соки­ми при­виле­ги­ями | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.007:   * Т1 (Т1.9; Т1.16); * Т2 (Т2.6); * Т3 (Т3.5); * Т6 (Т6.2; Т6.3) |
| УБИ.008 | Уг­ро­за вос­ста­нов­ле­ния и/или пов­торно­го ис­поль­зо­вания а­утен­ти­фика­ци­он­ной ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение, Учет­ные дан­ные поль­зо­вате­ля | НП.7; НП.9; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.008:   * Т1 (Т1.6); * Т2 (Т2.10); * Т4 (Т4.1) |
| УБИ.009 | Уг­ро­за вос­ста­нов­ле­ния пре­дыду­щей у­яз­ви­мой вер­сии BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.009:   * Т1 (Т1.9); * Т3 (T3.18); * Т4 (T4.8) |
| УБИ.010 | Уг­ро­за вы­хода про­цес­са за пре­делы вир­ту­аль­ной ма­шины | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.010:   * Т1 (Т1.5; Т1.9; Т1.16; T1.22); * Т2 (Т2.5; Т2.6); * Т3 (Т3.1; Т3.2) |
| УБИ.012 | Уг­ро­за дес­трук­тивно­го из­ме­нения кон­фи­гура­ции/сре­ды ок­ру­жения прог­рамм | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Объ­ек­ты фай­ло­вой сис­те­мы, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.012:   * Т1 (Т1.9; Т1.16); * Т2 (Т2.5; Т2.6); * Т3 (Т3.7) |
| УБИ.013 | Уг­ро­за дес­трук­тивно­го ис­поль­зо­вания дек­ла­риро­ван­но­го фун­кци­она­ла BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.013:   * Т1 (Т1.9; Т1.16); * Т2 (Т2.5); * Т4 (Т4.6) |
| УБИ.014 | Уг­ро­за дли­тель­но­го удер­жа­ния вы­чис­ли­тель­ных ре­сур­сов поль­зо­вате­лями | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки, Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.014:   * Т1 (Т1.5; Т1.16; Т1.19); * Т2 (Т2.5; Т2.6) |
| УБИ.015 | Уг­ро­за дос­ту­па к за­щища­емым фай­лам с ис­поль­зо­вани­ем об­ходно­го пу­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы | НП.7; НП.9; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.015:   * Т1 (Т1.9; Т1.16); * Т2 (Т2.3; Т2.5; Т2.6); * Т6 (Т6.3; Т6.6) |
| УБИ.016 | Уг­ро­за дос­ту­па к ло­каль­ным фай­лам сер­ве­ра при по­мощи URL | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.016:   * Т1 (Т1.11; Т1.16); * Т2 (Т2.8); * Т6 (Т6.1) |
| УБИ.018 | Уг­ро­за заг­рузки неш­татной опе­раци­он­ной сис­те­мы | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.018:   * Т2 (Т2.5); * Т10 (Т10.2) |
| УБИ.019 | Уг­ро­за за­раже­ния DNS-ке­ша | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.019:   * Т1 (Т1.7); * Т2 (Т2.3; Т2.4); * Т8 (Т8.8) |
| УБИ.022 | Уг­ро­за из­бы­точ­но­го вы­деле­ния опе­ратив­ной па­мяти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.2; СР.4 | Сце­нарий ре­али­зации УБИ.022:   * Т2 (Т2.3; Т2.4; Т2.5); * Т3 (Т3.2; Т3.3) |
| УБИ.023 | Уг­ро­за из­ме­нения ком­по­нен­тов ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мы | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение, Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.1; НП.7; НП.9; НП.12; НП.13; НП.15; НП.16; НП.17; НП.19; НП.20; НП.21; НП.22; НП.23 | СР.1; СР.4 | Сце­нарий ре­али­зации УБИ.023:   * Т2 (Т2.7); * Т3 (Т3.7); * Т10 (Т10.3) |
| УБИ.025 | Уг­ро­за из­ме­нения сис­темных и гло­баль­ных пе­ремен­ных | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1 | Сце­нарий ре­али­зации УБИ.025:   * Т10 (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, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.027:   * Т3 (Т3.2); * Т8 (Т8.1) |
| УБИ.028 | Уг­ро­за ис­поль­зо­вания аль­тер­на­тив­ных пу­тей дос­ту­па к ре­сур­сам | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы | НП.7; НП.9; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.028:   * Т1 (Т1.5; Т1.9); * Т10 (Т10.1) |
| УБИ.030 | Уг­ро­за ис­поль­зо­вания ин­форма­ции иден­ти­фика­ции/а­утен­ти­фика­ции, за­дан­ной по умол­ча­нию | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение, Средс­тво за­щиты ин­форма­ции | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22; НП.24 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.030:   * Т1 (T1.1; Т1.9; Т1.16); * Т2 (Т2.4) |
| УБИ.031 | Уг­ро­за ис­поль­зо­вания ме­ханиз­мов ав­то­риза­ции для по­выше­ния при­виле­гий | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.8 | Сце­нарий ре­али­зации УБИ.031:   * Т1 (Т1.5; Т1.9; Т1.16); * Т2 (Т2.4; Т2.5); * Т6 (Т6.3; Т6.6) |
| УБИ.032 | Уг­ро­за ис­поль­зо­вания под­дель­ных циф­ро­вых под­пи­сей BIOS | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.032:   * Т1 (Т1.16); * Т2 (Т2.12); * Т3 (Т3.8; Т3.11); * Т4 (Т4.6) |
| УБИ.033 | Уг­ро­за ис­поль­зо­вания сла­бос­тей ко­диро­вания вход­ных дан­ных | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.033:   * Т1 (Т1.5); * Т2 (Т2.5; Т2.6); * Т10 (Т10.2) |
| УБИ.034 | Уг­ро­за ис­поль­зо­вания сла­бос­тей про­токо­лов се­тево­го/ло­каль­но­го об­ме­на дан­ны­ми | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Сис­темное прог­рам­мное обес­пе­чение | НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.034:   * Т1 (Т1.5; Т1.9); * Т2 (Т2.3; Т2.5); * Т10 (Т10.1) |
| УБИ.036 | Уг­ро­за ис­сле­дова­ния ме­ханиз­мов ра­боты прог­раммы | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.8 | Сце­нарий ре­али­зации УБИ.036:   * Т2 (Т2.5) |
| УБИ.037 | Уг­ро­за ис­сле­дова­ния при­ложе­ния че­рез от­чё­ты об ошиб­ках | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.037:   * Т1 (Т1.9); * Т2 (Т2.5; Т2.6) |
| УБИ.039 | Уг­ро­за ис­черпа­ния за­паса клю­чей, не­об­хо­димых для об­новле­ния BIOS | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.039:   * Т1 (Т1.5); * Т2 (Т2.5); * Т4 (Т4.6) |
| УБИ.041 | Уг­ро­за меж­сай­то­вого скрип­тинга | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Веб-сайт, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21; НП.22; НП.24 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.041:   * Т1 (T1.1; Т1.5; Т1.8); * Т2 (Т2.1); * Т3 (Т3.3) |
| УБИ.042 | Уг­ро­за меж­сай­то­вой под­делки зап­ро­са | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.2; СР.4 | Сце­нарий ре­али­зации УБИ.042:   * Т1 (T1.1; Т1.5; Т1.8); * Т2 (Т2.5); * Т3 (Т3.1; Т3.3; Т3.9) |
| УБИ.044 | Уг­ро­за на­руше­ния изо­ляции поль­зо­ватель­ских дан­ных внут­ри вир­ту­аль­ной ма­шины | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.044:   * Т1 (Т1.5; Т1.9; Т1.16); * Т2 (Т2.3; Т2.5); * Т3 (Т3.1); * Т10 (Т10.2; Т10.3) |
| УБИ.045 | Уг­ро­за на­руше­ния изо­ляции сре­ды ис­полне­ния BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.045:   * Т1 (Т1.5; Т1.9; Т1.16); * Т2 (Т2.5); * Т4 (Т4.6); * Т10 (Т10.2; Т10.6) |
| УБИ.046 | Уг­ро­за на­руше­ния про­цеду­ры а­утен­ти­фика­ции субъ­ек­тов вир­ту­аль­но­го ин­форма­ци­он­но­го вза­имо­дей­ствия | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.046:   * Т2 (Т2.4; Т2.5) |
| УБИ.048 | Уг­ро­за на­руше­ния тех­но­логии об­ра­бот­ки ин­форма­ции пу­тём не­сан­кци­они­рован­но­го вне­сения из­ме­нений в об­ра­зы вир­ту­аль­ных ма­шин | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.048:   * Т2 (Т2.3; Т2.5); * Т3 (Т3.7); * Т4 (Т4.3; Т4.5; Т4.7); * Т10 (Т10.2; Т10.7) |
| УБИ.049 | Уг­ро­за на­руше­ния це­лос­тнос­ти дан­ных ке­ша | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.049:   * Т2 (Т2.5); * Т3 (Т3.9); * Т10 (Т10.1; Т10.2) |
| 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, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.9 | Сце­нарий ре­али­зации УБИ.051:   * Т10 (Т10.8) |
| УБИ.053 | Уг­ро­за не­воз­можнос­ти уп­равле­ния пра­вами поль­зо­вате­лей BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.11 | Сце­нарий ре­али­зации УБИ.053:   * Т2 (Т2.5) |
| УБИ.058 | Уг­ро­за не­кон­тро­лиру­емо­го рос­та чис­ла вир­ту­аль­ных ма­шин | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тва уда­лен­но­го ад­ми­нис­три­рова­ния ин­форма­ци­он­ной (ав­то­мати­зиро­ван­ной) сис­те­мой или ее ком­по­нен­та­ми, фун­кци­они­ру­ющи­ми в об­лачной сис­те­ме | НП.12; НП.15; НП.16 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.058:   * Т10 (Т10.10) |
| УБИ.059 | Уг­ро­за не­кон­тро­лиру­емо­го рос­та чис­ла за­резер­ви­рован­ных вы­чис­ли­тель­ных ре­сур­сов | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.059:   * Т1 (T1.4; Т1.5; Т1.6; Т1.11; Т1.15); * Т2 (Т2.2; Т2.8); * Т10 (Т10.10) |
| УБИ.061 | Уг­ро­за не­кор­рек­тно­го за­дания струк­ту­ры дан­ных тран­закции | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ба­за дан­ных, Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик | НП.2; НП.4; НП.5; НП.6; НП.7; НП.9; НП.10; НП.11; НП.12; НП.13; НП.14; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.061:   * Т1 (Т1.5); * Т2 (Т2.5) |
| УБИ.062 | Уг­ро­за не­кор­рек­тно­го ис­поль­зо­вания проз­рачно­го прок­си-сер­ве­ра за счёт пла­гинов бра­узе­ра | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.2; СР.9 | Сце­нарий ре­али­зации УБИ.062:   * Т1 (Т1.5); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.063 | Уг­ро­за не­кор­рек­тно­го ис­поль­зо­вания фун­кци­она­ла прог­рам­мно­го и ап­па­рат­но­го обес­пе­чения | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.063:   * Т2 (Т2.5); * Т10 (Т10.11) |
| УБИ.064 | Уг­ро­за не­кор­рек­тной ре­али­зации по­лити­ки ли­цен­зи­рова­ния в об­ла­ке | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма или ее ком­по­нен­ты, фун­кци­они­ру­ющие в об­лачной сис­те­ме | НП.1; НП.8; НП.12; НП.13; НП.15; НП.16 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.064:   * Т1 (T1.1); * Т10 (Т10.10) |
| УБИ.067 | Уг­ро­за неп­ра­вомер­но­го оз­на­ком­ле­ния с за­щища­емой ин­форма­цией | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | За­щища­емая ин­форма­ция | НП.2; НП.3; НП.4; НП.5; НП.6; НП.7; НП.8; НП.9; НП.11; НП.14; НП.17; НП.19 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.067:   * Т1 (Т1.13; Т1.14); * Т10 (Т10.1) |
| УБИ.068 | Уг­ро­за неп­ра­вомер­но­го/не­кор­рек­тно­го ис­поль­зо­вания ин­терфей­са вза­имо­дей­ствия с при­ложе­ни­ем | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.068:   * Т1 (Т1.5); * Т2 (Т2.5); * Т10 (Т10.3) |
| УБИ.069 | Уг­ро­за неп­ра­вомер­ных дей­ствий в ка­налах свя­зи | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевой тра­фик | НП.2; НП.6; НП.7; НП.9; НП.16; НП.17; НП.19; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.069:   * Т1 (Т1.5); * Т2 (Т2.5); * Т10 (Т10.8) |
| УБИ.071 | Уг­ро­за не­сан­кци­они­рован­но­го вос­ста­нов­ле­ния уда­лён­ной за­щища­емой ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.071:   * Т1 (Т1.9); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.072 | Уг­ро­за не­сан­кци­они­рован­но­го вык­лю­чения или об­хо­да ме­ханиз­ма за­щиты от за­писи в BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.2; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.072:   * Т2 (Т2.5); * Т3 (Т3.8; T3.18); * Т4 (Т4.6) |
| 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, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой), Мик­ропрог­рам­мное обес­пе­чение, Се­тевое обо­рудо­вание, Се­тевое прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21; НП.24 | СР.1; СР.2; СР.9 | Сце­нарий ре­али­зации УБИ.073:   * Т1 (Т1.5); * Т2 (Т2.5); * Т4 (Т4.6) |
| УБИ.074 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к а­утен­ти­фика­ци­он­ной ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки, Объ­ек­ты фай­ло­вой сис­те­мы, Сис­темное прог­рам­мное обес­пе­чение, Учет­ные дан­ные поль­зо­вате­ля | НП.7; НП.9; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.074:   * Т1 (Т1.12); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.075 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к вир­ту­аль­ным ка­налам пе­реда­чи | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.075:   * Т1 (Т1.5); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.076 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к ги­пер­ви­зору из вир­ту­аль­ной ма­шины и (или) фи­зичес­кой се­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.076:   * Т1 (T1.3; Т1.6; Т1.9; Т1.11; Т1.15); * Т2 (Т2.8; Т2.11); * Т10 (Т10.10) |
| УБИ.077 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к дан­ным за пре­дела­ми за­резер­ви­рован­но­го ад­ресно­го прос­транс­тва, в том чис­ле вы­делен­но­го под вир­ту­аль­ное ап­па­рат­ное обес­пе­чение | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.077:   * Т1 (Т1.5); * Т2 (Т2.5); * Т3 (Т3.1); * Т4 (Т4.3); * Т7 (Т7.18); * Т10 (Т10.1; Т10.11) |
| УБИ.078 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емым вир­ту­аль­ным ма­шинам из вир­ту­аль­ной и (или) фи­зичес­кой се­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.078:   * Т1 (Т1.5); * Т2 (Т2.4; Т2.5); * Т10 (Т10.1; Т10.2) |
| УБИ.079 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емым вир­ту­аль­ным ма­шинам со сто­роны дру­гих вир­ту­аль­ных ма­шин | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.079:   * Т1 (Т1.5); * Т2 (Т2.4; Т2.5); * Т10 (Т10.1; Т10.2) |
| УБИ.080 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емым вир­ту­аль­ным ус­трой­ствам из вир­ту­аль­ной и (или) фи­зичес­кой се­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.080:   * Т1 (Т1.5; Т1.16); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.084 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к сис­те­ме хра­нения дан­ных из вир­ту­аль­ной и (или) фи­зичес­кой се­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.084:   * Т1 (Т1.5; T1.22) |
| УБИ.085 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к хра­нимой в вир­ту­аль­ном прос­транс­тве за­щища­емой ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | За­щища­емая ин­форма­ция | НП.2; НП.3; НП.4; НП.5; НП.6; НП.7; НП.8; НП.9; НП.11; НП.14; НП.17; НП.19 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.085:   * Т1 (Т1.5; Т1.9); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.086 | Уг­ро­за не­сан­кци­они­рован­но­го из­ме­нения а­утен­ти­фика­ци­он­ной ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы, Учет­ные дан­ные поль­зо­вате­ля | НП.7; НП.9; НП.12; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.086:   * Т1 (Т1.5; Т1.12; T1.22); * Т2 (Т2.4; Т2.11); * Т4 (Т4.1); * Т10 (Т10.1) |
| УБИ.087 | Уг­ро­за не­сан­кци­они­рован­но­го ис­поль­зо­вания при­виле­гиро­ван­ных фун­кций BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.087:   * Т1 (Т1.5; Т1.9; Т1.16); * Т2 (Т2.5) |
| УБИ.088 | Уг­ро­за не­сан­кци­они­рован­но­го ко­пиро­вания за­щища­емой ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | За­щища­емая ин­форма­ция, Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки, Объ­ек­ты фай­ло­вой сис­те­мы | НП.2; НП.3; НП.4; НП.5; НП.6; НП.7; НП.8; НП.9; НП.11; НП.12; НП.13; НП.14; НП.15; НП.16; НП.17; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.088:   * Т2 (Т2.4; Т2.9); * Т10 (Т10.1) |
| УБИ.089 | Уг­ро­за не­сан­кци­они­рован­но­го ре­дак­ти­рова­ния ре­ес­тра | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.089:   * Т1 (Т1.5; Т1.9); * Т2 (Т2.4); * Т4 (Т4.5); * Т10 (Т10.1) |
| УБИ.090 | Уг­ро­за не­сан­кци­они­рован­но­го соз­да­ния учёт­ной за­писи поль­зо­вате­ля | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.090:   * Т1 (Т1.5); * Т2 (Т2.4); * Т4 (Т4.1); * Т5 (Т5.2); * Т10 (Т10.2) |
| УБИ.091 | Уг­ро­за не­сан­кци­они­рован­но­го уда­ления за­щища­емой ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | За­щища­емая ин­форма­ция, Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки, Объ­ек­ты фай­ло­вой сис­те­мы | НП.2; НП.3; НП.4; НП.5; НП.6; НП.7; НП.8; НП.9; НП.11; НП.12; НП.13; НП.14; НП.15; НП.16; НП.17; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.091:   * Т1 (Т1.5); * Т2 (Т2.5); * Т10 (Т10.8) |
| УБИ.093 | Уг­ро­за не­сан­кци­они­рован­но­го уп­равле­ния бу­фером | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1 | Сце­нарий ре­али­зации УБИ.093:   * Т1 (Т1.9); * Т2 (Т2.4; Т2.5); * Т3 (Т3.2); * Т10 (Т10.1) |
| УБИ.094 | Уг­ро­за не­сан­кци­они­рован­но­го уп­равле­ния син­хро­низа­цией и сос­то­яни­ем | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.094:   * Т1 (Т1.5); * Т2 (Т2.5); * Т10 (Т10.1; Т10.3) |
| УБИ.095 | Уг­ро­за не­сан­кци­они­рован­но­го уп­равле­ния ука­зате­лями | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.095:   * Т1 (Т1.5); * Т2 (Т2.4; Т2.11); * Т3 (Т3.2); * Т10 (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, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.098:   * Т1 (T1.4; Т1.5; T1.22); * Т2 (Т2.3); * Т10 (Т10.1) |
| УБИ.099 | Уг­ро­за об­на­руже­ния хос­тов | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.099:   * Т1 (T1.4; Т1.5; T1.22); * Т2 (Т2.3); * Т10 (Т10.1) |
| УБИ.100 | Уг­ро­за об­хо­да не­кор­рек­тно нас­тро­ен­ных ме­ханиз­мов а­утен­ти­фика­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.100:   * Т2 (Т2.4; Т2.5); * Т4 (Т4.1); * Т6 (Т6.6) |
| УБИ.102 | Уг­ро­за опос­ре­дован­но­го уп­равле­ния груп­пой прог­рамм че­рез сов­мес­тно ис­поль­зу­емые дан­ные | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.102:   * Т2 (Т2.5) |
| УБИ.103 | Уг­ро­за оп­ре­деле­ния ти­пов объ­ек­тов за­щиты | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.103:   * Т1 (T1.1; T1.3); * Т2 (Т2.4) |
| УБИ.104 | Уг­ро­за оп­ре­деле­ния то­поло­гии вы­чис­ли­тель­ной се­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.104:   * Т1 (T1.4; Т1.5; T1.22); * Т2 (Т2.3) |
| УБИ.108 | Уг­ро­за ошиб­ки об­новле­ния ги­пер­ви­зора | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.108:   * Т2 (Т2.5); * Т10 (Т10.2) |
| УБИ.109 | Уг­ро­за пе­ребо­ра всех нас­тро­ек и па­рамет­ров при­ложе­ния | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.109:   * Т2 (Т2.5; Т2.6); * Т10 (Т10.10) |
| УБИ.111 | Уг­ро­за пе­реда­чи дан­ных по скры­тым ка­налам | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевой тра­фик, Сис­темное прог­рам­мное обес­пе­чение | НП.2; НП.6; НП.7; НП.9; НП.12; НП.13; НП.15; НП.16; НП.17; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.111:   * Т2 (Т2.4); * Т9 (Т9.10; Т9.12) |
| УБИ.113 | Уг­ро­за пе­резаг­рузки ап­па­рат­ных и прог­рам­мно-ап­па­рат­ных средств вы­чис­ли­тель­ной тех­ни­ки | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.22; НП.23 | СР.1 | Сце­нарий ре­али­зации УБИ.113:   * Т2 (Т2.5; Т2.11); * Т10 (Т10.8) |
| УБИ.114 | Уг­ро­за пе­репол­не­ния це­лочис­ленных пе­ремен­ных | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1 | Сце­нарий ре­али­зации УБИ.114:   * Т1 (T1.1; Т1.5; Т1.9); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.115 | Уг­ро­за пе­рех­ва­та вво­димой и вы­води­мой на пе­рифе­рий­ные ус­трой­ства ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.12; НП.13; НП.15; НП.16; НП.17; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.115:   * Т1 (T1.4; Т1.12); * Т2 (Т2.4; Т2.5; Т2.11); * Т3 (Т3.1); * Т4 (Т4.1); * Т10 (Т10.1; Т10.3) |
| УБИ.116 | Уг­ро­за пе­рех­ва­та дан­ных, пе­реда­ва­емых по вы­чис­ли­тель­ной се­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевой тра­фик | НП.2; НП.6; НП.7; НП.9; НП.16; НП.17; НП.19; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.116:   * Т1 (T1.3); * Т2 (Т2.4; Т2.5; Т2.11) |
| УБИ.117 | Уг­ро­за пе­рех­ва­та при­виле­гиро­ван­но­го по­тока | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1 | Сце­нарий ре­али­зации УБИ.117:   * Т1 (Т1.5); * Т2 (Т2.4; Т2.5; Т2.11); * Т6 (Т6.1); * Т10 (Т10.1) |
| УБИ.118 | Уг­ро­за пе­рех­ва­та при­виле­гиро­ван­но­го про­цес­са | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1 | Сце­нарий ре­али­зации УБИ.118:   * Т1 (Т1.5); * Т2 (Т2.4; Т2.5; Т2.11); * Т3 (Т3.1); * Т4 (Т4.1); * Т6 (Т6.3) |
| УБИ.119 | Уг­ро­за пе­рех­ва­та уп­равле­ния ги­пер­ви­зором | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.119:   * Т1 (Т1.5); * Т2 (Т2.5; Т2.11); * Т10 (Т10.1) |
| УБИ.120 | Уг­ро­за пе­рех­ва­та уп­равле­ния сре­дой вир­ту­али­зации | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Вир­ту­аль­ная ин­фраструк­ту­ра (воз­дей­ствие на ги­пер­ви­зор, вир­ту­аль­ные ма­шины, об­ра­зы вир­ту­аль­ных ма­шин, вир­ту­аль­ные ус­трой­ства, вир­ту­аль­ные дис­ки и вир­ту­аль­ные ус­трой­ства хра­нения дан­ных, сис­те­му уп­равле­ния вир­ту­аль­ной ин­фраструк­ту­рой) | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.120:   * Т1 (Т1.5); * Т2 (Т2.5; Т2.11); * Т10 (Т10.1) |
| УБИ.121 | Уг­ро­за пов­режде­ния сис­темно­го ре­ес­тра | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы | НП.7; НП.9; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.121:   * Т2 (Т2.4; Т2.5; Т2.11); * Т10 (Т10.8; Т10.10) |
| УБИ.122 | Уг­ро­за по­выше­ния при­виле­гий | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.122:   * Т2 (Т2.5); * Т3 (Т3.5); * Т6 (Т6.1); * Т10 (Т10.3) |
| УБИ.123 | Уг­ро­за под­бо­ра па­роля BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.123:   * Т1 (Т1.6); * Т2 (Т2.5; Т2.10); * Т4 (Т4.1); * Т10 (Т10.1) |
| УБИ.124 | Уг­ро­за под­делки за­писей жур­на­ла ре­гис­тра­ции со­бытий | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение, Средс­тво за­щиты ин­форма­ции | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22; НП.24 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.124:   * Т1 (T1.22); * Т2 (Т2.5; Т2.11); * Т7 (Т7.6) |
| УБИ.127 | Уг­ро­за под­ме­ны дей­ствия поль­зо­вате­ля пу­тём об­ма­на | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.127:   * Т1 (Т1.11); * Т2 (Т2.8; Т2.11) |
| УБИ.128 | Уг­ро­за под­ме­ны до­верен­но­го поль­зо­вате­ля | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.128:   * Т1 (Т1.5); * Т2 (Т2.5; Т2.9) |
| УБИ.129 | Уг­ро­за под­ме­ны ре­зер­вной ко­пии прог­рам­мно­го обес­пе­чения BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.129:   * Т1 (Т1.5); * Т2 (Т2.5); * Т3 (Т3.7); * Т4 (Т4.6; Т4.7) |
| УБИ.130 | Уг­ро­за под­ме­ны со­дер­жи­мого се­тевых ре­сур­сов | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.130:   * Т1 (Т1.5); * Т2 (Т2.5; Т2.11); * Т10 (Т10.2) |
| УБИ.131 | Уг­ро­за под­ме­ны субъ­ек­та се­тево­го дос­ту­па | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1 | Сце­нарий ре­али­зации УБИ.131:   * Т1 (T1.2); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.132 | Уг­ро­за по­луче­ния пред­ва­ритель­ной ин­форма­ции об объ­ек­те за­щиты | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.132:   * Т1 (Т1.5; Т1.6; Т1.17) |
| УБИ.139 | Уг­ро­за пре­одо­ления фи­зичес­кой за­щиты | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое обо­рудо­вание, Средс­тво вы­чис­ли­тель­ной тех­ни­ки, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21; НП.22; НП.23; НП.24 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.139:   * Т1 (Т1.13); * Т2 (Т2.2) |
| УБИ.140 | Уг­ро­за при­веде­ния сис­те­мы в сос­то­яние «от­каз в об­слу­жива­нии» | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Сис­темное прог­рам­мное обес­пе­чение, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.9; СР.12 | Сце­нарий ре­али­зации УБИ.140:   * Т2 (Т2.3; Т2.5); * Т10 (Т10.10) |
| УБИ.143 | Уг­ро­за прог­рам­мно­го вы­веде­ния из строя средств хра­нения, об­ра­бот­ки и (или) вво­да/вы­вода/пе­реда­чи ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки, Мик­ропрог­рам­мное обес­пе­чение, Се­тевое обо­рудо­вание | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21; НП.24 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.143:   * Т1 (Т1.5); * Т2 (Т2.5); * Т7 (Т7.8); * Т10 (Т10.10) |
| УБИ.144 | Уг­ро­за прог­рам­мно­го сбро­са па­роля BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.144:   * Т1 (Т1.9; T1.22); * Т2 (Т2.4; Т2.11); * Т10 (Т10.6) |
| УБИ.145 | Уг­ро­за про­пус­ка про­вер­ки це­лос­тнос­ти прог­рам­мно­го обес­пе­чения | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.145:   * Т2 (Т2.4; Т2.5; Т2.8); * Т3 (Т3.3) |
| УБИ.149 | Уг­ро­за сбоя об­ра­бот­ки спе­ци­аль­ным об­ра­зом из­ме­нён­ных фай­лов | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы, Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.9; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.4 | Сце­нарий ре­али­зации УБИ.149:   * Т1 (Т1.5); * Т2 (Т2.5); * Т10 (Т10.10) |
| УБИ.150 | Уг­ро­за сбоя про­цес­са об­новле­ния BIOS | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.9 | Сце­нарий ре­али­зации УБИ.150:   * Т1 (Т1.5); * Т2 (Т2.5); * Т4 (Т4.6) |
| УБИ.151 | Уг­ро­за ска­ниро­вания веб-сер­ви­сов, раз­ра­ботан­ных на ос­но­ве язы­ка опи­сания WSDL | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Веб-сер­вер | НП.10; НП.12; НП.15; НП.16; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.151:   * Т1 (Т1.5; T1.22); * Т2 (Т2.3; Т2.5) |
| УБИ.152 | Уг­ро­за уда­ления а­утен­ти­фика­ци­он­ной ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение, Учет­ные дан­ные поль­зо­вате­ля | НП.7; НП.9; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.152:   * Т1 (T1.22); * Т2 (Т2.4; Т2.11); * Т10 (Т10.10) |
| УБИ.153 | Уг­ро­за уси­ления воз­дей­ствия на вы­чис­ли­тель­ные ре­сур­сы поль­зо­вате­лей при по­мощи сто­рон­них сер­ве­ров | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.153:   * Т1 (T1.2; T1.22); * Т2 (Т2.3; Т2.5) |
| УБИ.154 | Уг­ро­за ус­та­нов­ки у­яз­ви­мых вер­сий об­новле­ния прог­рам­мно­го обес­пе­чения BIOS | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | BIOS/UEFI | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.154:   * Т1 (Т1.5); * Т2 (Т2.5); * Т3 (Т3.8); * Т4 (Т4.6); * Т7 (Т7.22); * Т10 (Т10.6; Т10.10) |
| УБИ.155 | Уг­ро­за ут­ра­ты вы­чис­ли­тель­ных ре­сур­сов | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки, Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Сис­темное прог­рам­мное обес­пе­чение, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.155:   * Т1 (Т1.5; Т1.9); * Т2 (Т2.3; Т2.5; Т2.11); * Т10 (Т10.10) |
| УБИ.156 | Уг­ро­за ут­ра­ты но­сите­лей ин­форма­ции | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.156:   * Т1 (Т1.10); * Т10 (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, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое обо­рудо­вание, Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21; НП.22; НП.23; НП.24 | СР.1; СР.9; СР.11 | Сце­нарий ре­али­зации УБИ.157:   * Т2 (Т2.2); * Т10 (Т10.8; Т10.10) |
| УБИ.158 | Уг­ро­за фор­ма­тиро­вания но­сите­лей ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.158:   * Т2 (Т2.2; Т2.5); * Т10 (Т10.8) |
| УБИ.159 | Уг­ро­за «фор­си­рован­но­го веб-бра­узин­га» | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.159:   * Т2 (Т2.1; Т2.5); * Т10 (Т10.1) |
| УБИ.160 | Уг­ро­за хи­щения средств хра­нения, об­ра­бот­ки и (или) вво­да/вы­вода/пе­реда­чи ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ма­шин­ный но­ситель ин­форма­ции в сос­та­ве средств вы­чис­ли­тель­ной тех­ни­ки, Се­тевое обо­рудо­вание, Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21; НП.22; НП.23; НП.24 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.160:   * Т2 (Т2.5) |
| УБИ.162 | Уг­ро­за экс­плу­ата­ции циф­ро­вой под­пи­си прог­рам­мно­го ко­да | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.4 | Сце­нарий ре­али­зации УБИ.162:   * Т1 (Т1.10); * Т3 (Т3.11; Т3.13; Т3.16) |
| УБИ.163 | Уг­ро­за пе­рех­ва­та ис­клю­чения/сиг­на­ла из при­виле­гиро­ван­но­го бло­ка фун­кций | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.163:   * Т1 (T1.3); * Т2 (Т2.5); * Т10 (Т10.1) |
| УБИ.165 | Уг­ро­за вклю­чения в про­ект не дос­то­вер­но ис­пы­тан­ных ком­по­нен­тов | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | НП.1; НП.8; НП.12; НП.13; НП.15; НП.16 | СР.9 | Сце­нарий ре­али­зации УБИ.165:   * Т2 (Т2.5) |
| УБИ.166 | Уг­ро­за внед­ре­ния сис­темной из­бы­точ­ности | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | НП.1; НП.8; НП.12; НП.13; НП.15; НП.16 | СР.9 | Сце­нарий ре­али­зации УБИ.166:   * Т2 (Т2.5) |
| УБИ.167 | Уг­ро­за за­раже­ния компь­юте­ра при по­сеще­нии неб­ла­гона­дёж­ных сай­тов | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.167:   * Т2 (Т2.4); * Т3 (Т3.3) |
| УБИ.168 | Уг­ро­за «кра­жи» учёт­ной за­писи дос­ту­па к се­тевым сер­ви­сам | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Учет­ные дан­ные поль­зо­вате­ля | НП.7; НП.9; НП.10; НП.12; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.168:   * Т1 (T1.3; Т1.6; Т1.9; Т1.11; Т1.15); * Т2 (Т2.8; Т2.11); * Т4 (Т4.1) |
| УБИ.169 | Уг­ро­за на­личия ме­ханиз­мов раз­ра­бот­чи­ка | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.169:   * Т2 (Т2.5; Т2.6); * Т3 (Т3.12) |
| УБИ.170 | Уг­ро­за неп­ра­вомер­но­го шиф­ро­вания ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы | НП.7; НП.9; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.4 | Сце­нарий ре­али­зации УБИ.170:   * Т2 (Т2.4); * Т3 (Т3.3); * Т10 (Т10.8) |
| УБИ.171 | Уг­ро­за скрыт­но­го вклю­чения вы­чис­ли­тель­но­го ус­трой­ства в сос­тав бот-се­ти | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.21 | СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.171:   * Т1 (T1.2); * Т2 (Т2.3; Т2.4; Т2.5); * Т3 (Т3.1); * Т4 (Т4.3) |
| УБИ.172 | Уг­ро­за рас­простра­нения «поч­то­вых чер­вей» | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.172:   * Т1 (T1.1); * Т2 (Т2.3) |
| УБИ.173 | Уг­ро­за «спа­ма» веб-сер­ве­ра | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Веб-сер­вер | НП.10; НП.12; НП.15; НП.16; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.173:   * Т1 (T1.1); * Т2 (Т2.1) |
| УБИ.174 | Уг­ро­за «фар­минга» | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.174:   * Т1 (T1.1; Т1.8); * Т3 (Т3.3) |
| УБИ.175 | Уг­ро­за «фи­шин­га» | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Се­тевой тра­фик, Узел вы­чис­ли­тель­ной се­ти (ав­то­мати­зиро­ван­ные ра­бочие мес­та, сер­ве­ра, мар­шру­тиза­торы, ком­му­тато­ры, IoT-ус­трой­ства и т.п.) | НП.1; НП.2; НП.6; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.175:   * Т1 (T1.1; Т1.11); * Т2 (Т2.8) |
| 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, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тво за­щиты ин­форма­ции | НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.24 | СР.1; СР.8; СР.12 | Сце­нарий ре­али­зации УБИ.176:   * Т1 (T1.4; Т1.5); * Т2 (Т2.3; Т2.5); * Т10 (Т10.3; Т10.10) |
| УБИ.177 | Уг­ро­за не­под­тверждён­но­го вво­да дан­ных опе­рато­ром в сис­те­му, свя­зан­ную с бе­зопас­ностью | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.177:   * Т10 (Т10.14) |
| УБИ.178 | Уг­ро­за не­сан­кци­они­рован­но­го ис­поль­зо­вания сис­темных и се­тевых ути­лит | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1 | Сце­нарий ре­али­зации УБИ.178:   * Т2 (Т2.4; Т2.5); * Т10 (Т10.5) |
| УБИ.179 | Уг­ро­за не­сан­кци­они­рован­ной мо­дифи­кации за­щища­емой ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Объ­ек­ты фай­ло­вой сис­те­мы | НП.7; НП.9; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.8; СР.11 | Сце­нарий ре­али­зации УБИ.179:   * Т2 (Т2.5); * Т10 (Т10.7; Т10.8) |
| УБИ.180 | Уг­ро­за от­ка­за под­систе­мы обес­пе­чения тем­пе­ратур­но­го ре­жима | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Сис­те­ма под­держа­ния тем­пе­ратур­но-влаж­нос­тно­го ре­жима | НП.12; НП.13; НП.15; НП.16; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.180:   * Т1 (Т1.9; Т1.11); * Т2 (Т2.8); * Т10 (Т10.14) |
| УБИ.182 | Уг­ро­за фи­зичес­ко­го ус­та­рева­ния ап­па­рат­ных ком­по­нен­тов | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое обо­рудо­вание, Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21; НП.22; НП.23; НП.24 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.182:   * Т10 (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, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тво за­щиты ин­форма­ции | НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.24 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.185:   * Т2 (Т2.4); * Т7 (Т7.4) |
| УБИ.186 | Уг­ро­за внед­ре­ния вре­донос­но­го ко­да че­рез рек­ла­му, сер­ви­сы и кон­тент | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.186:   * Т1 (T1.1); * Т3 (Т3.3) |
| УБИ.187 | Уг­ро­за не­сан­кци­они­рован­но­го воз­дей­ствия на средс­тво за­щиты ин­форма­ции | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тво за­щиты ин­форма­ции | НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.24 | СР.1; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.187:   * Т2 (Т2.4); * Т7 (Т7.4); * Т10 (Т10.2) |
| УБИ.188 | Уг­ро­за под­ме­ны прог­рам­мно­го обес­пе­чения | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.2; СР.9 | Сце­нарий ре­али­зации УБИ.188:   * Т2 (Т2.7); * Т3 (Т3.7; Т3.8; Т3.10); * Т7 (Т7.24); * Т10 (Т10.7) |
| УБИ.189 | Уг­ро­за мас­ки­рова­ния дей­ствий вре­донос­но­го ко­да | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.1; СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.189:   * Т2 (Т2.4); * Т3 (Т3.7); * Т7 (Т7.1) |
| УБИ.190 | Уг­ро­за внед­ре­ния вре­донос­но­го ко­да за счет по­сеще­ния за­ражен­ных сай­тов в се­ти Ин­тернет | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое прог­рам­мное обес­пе­чение | НП.7; НП.10; НП.12; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21 | СР.2; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.190:   * Т1 (T1.1; Т1.8; Т1.11); * Т2 (Т2.1; Т2.4; Т2.8); * Т3 (Т3.3) |
| УБИ.191 | Уг­ро­за внед­ре­ния вре­донос­но­го ко­да в дис­три­бутив прог­рам­мно­го обес­пе­чения | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.2; СР.8; СР.9 | Сце­нарий ре­али­зации УБИ.191:   * Т2 (Т2.7); * Т3 (Т3.2) |
| УБИ.192 | Уг­ро­за ис­поль­зо­вания у­яз­ви­мых вер­сий прог­рам­мно­го обес­пе­чения | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.192:   * Т2 (Т2.5); * Т10 (Т10.2) |
| УБИ.198 | Уг­ро­за скрыт­ной ре­гис­тра­ции вре­донос­ной прог­раммой учет­ных за­писей ад­ми­нис­тра­торов | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.198:   * Т1 (Т1.5; Т1.6; Т1.12); * Т2 (Т2.6); * Т4 (Т4.1); * Т7 (Т7.12; Т7.13) |
| УБИ.203 | Уг­ро­за утеч­ки ин­форма­ции с не­под­клю­чен­ных к се­ти Ин­тернет компь­юте­ров | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Се­тевое обо­рудо­вание, Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.10; НП.12; НП.13; НП.15; НП.16; НП.18; НП.19; НП.20; НП.21; НП.22; НП.23; НП.24 | СР.1; СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.203:   * Т2 (Т2.5); * Т3 (Т3.2); * Т6 (Т6.3); * Т9 (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, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.22; НП.23 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.205:   * Т2 (Т2.4) |
| УБИ.208 | Уг­ро­за не­целе­вого ис­поль­зо­вания вы­чис­ли­тель­ных ре­сур­сов средс­тва вы­чис­ли­тель­ной тех­ни­ки | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.22; НП.23 | СР.2; СР.8 | Сце­нарий ре­али­зации УБИ.208:   * Т1 (Т1.5; Т1.11); * Т2 (Т2.7); * Т10 (Т10.11) |
| УБИ.209 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к за­щища­емой па­мяти яд­ра про­цес­со­ра | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.22; НП.23 | СР.1 | Сце­нарий ре­али­зации УБИ.209:   * Т1 (Т1.5; Т1.9); * Т2 (Т2.4); * Т10 (Т10.1; Т10.5) |
| УБИ.211 | Уг­ро­за ис­поль­зо­вания неп­ро­верен­ных поль­зо­ватель­ских дан­ных при фор­ми­рова­нии кон­фи­гура­ци­он­но­го фай­ла, ис­поль­зу­емо­го прог­рам­мным обес­пе­чени­ем ад­ми­нис­три­рова­ния ин­форма­ци­он­ных сис­тем | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Сис­темное прог­рам­мное обес­пе­чение | НП.7; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.211:   * Т10 (Т10.2) |
| УБИ.212 | Уг­ро­за пе­рех­ва­та уп­равле­ния ин­форма­ци­он­ной сис­те­мой | Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма, Сис­темное прог­рам­мное обес­пе­чение, Средс­тво вы­чис­ли­тель­ной тех­ни­ки | НП.1; НП.7; НП.8; НП.12; НП.13; НП.15; НП.16; НП.19; НП.20; НП.21; НП.22; НП.23 | СР.1 | Сце­нарий ре­али­зации УБИ.212:   * Т2 (Т2.4; Т2.5); * Т8 (Т8.1); * Т10 (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, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | НП.1; НП.8; НП.12; НП.13; НП.15; НП.16 | СР.1; СР.8 | Сце­нарий ре­али­зации УБИ.214:   * Т7 (Т7.4) |
| УБИ.215 | Уг­ро­за не­сан­кци­они­рован­но­го дос­ту­па к сис­те­ме при по­мощи сто­рон­них сер­ви­сов | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Ин­форма­ци­он­ная (ав­то­мати­зиро­ван­ная) сис­те­ма | НП.1; НП.8; НП.12; НП.13; НП.15; НП.16 | СР.1; СР.9 | Сце­нарий ре­али­зации УБИ.215:   * Т1 (Т1.5); * Т7 (Т7.25); * Т10 (Т10.2) |
| УБИ.217 | Уг­ро­за ис­поль­зо­вания ском­про­мети­рован­но­го до­верен­но­го ис­точни­ка об­новле­ний прог­рам­мно­го обес­пе­чения | Внеш­ний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внеш­ний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий ба­зовы­ми по­вышен­ны­ми воз­можнос­тя­ми, Внут­ренний на­руши­тель, об­ла­да­ющий сред­ни­ми воз­можнос­тя­ми | Мик­ропрог­рам­мное обес­пе­чение, Прик­ладное прог­рам­мное обес­пе­чение, Се­тевое прог­рам­мное обес­пе­чение, Сис­темное прог­рам­мное обес­пе­чение | НП.1; НП.7; НП.9; НП.10; НП.12; НП.13; НП.15; НП.16; НП.17; НП.18; НП.19; НП.20; НП.21; НП.22 | СР.1; СР.2 | Сце­нарий ре­али­зации УБИ.217:   * Т2 (Т2.7); * Т3 (Т3.8); * Т7 (Т7.24) |

Приложение № 7

Уточненные возможности нарушителей и направления атак

| № | **Уточ­нён­ные воз­мож­нос­ти на­ру­ши­те­лей и нап­рав­ле­ния атак (соот­ветствую­щие ак­туаль­ные уг­розы)** | **Ак­туаль­ность ис­поль­зо­ва­ния (при­ме­не­ния) для построения и реа­ли­за­ции атак** | **Обоснование** |
| --- | --- | --- | --- |
| 1.1 | Про­веде­ние ата­ки при на­хож­де­нии в пре­делах кон­тро­лиру­емой зо­ны | Да | * Об­слу­жива­ющий пер­со­нал и ли­ца, обес­пе­чива­ющие фун­кци­они­рова­ние ГИС в сфе­ре фи­нан­сов, не име­ют воз­можнос­ти на­ходить­ся в по­меще­ни­ях, где рас­по­ложе­на ГИС в сфе­ре фи­нан­сов, в от­сутс­твие поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов; * Ра­бота поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов и поль­зо­вате­лей крип­тосредств рег­ла­мен­ти­рова­на; * От­ветс­твен­ный за за­щиту ин­форма­ции, ад­ми­нис­тра­торы ГИС в сфе­ре фи­нан­сов наз­на­ча­ют­ся из чис­ла осо­бо до­верен­ных лиц; * Ре­монт, об­слу­жива­ние и соп­ро­вож­де­ние прог­рам­мных, тех­ни­чес­ких и прог­рам­мно-тех­ни­чес­ких средств ГИС в сфе­ре фи­нан­сов, в том чис­ле СЗИ, вы­пол­ня­ет­ся до­верен­ны­ми ли­цами, с вы­пол­не­ни­ем мер по за­щите ин­форма­ции; * В по­меще­ни­ях, в ко­торых про­ис­хо­дит об­ра­бот­ка за­щища­емой ин­форма­ции, не­воз­можно на­хож­де­ние пос­то­рон­них лиц; * Про­водит­ся обу­чение поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов ме­рам по за­щите ин­форма­ции и пре­дуп­режде­ние об от­ветс­твен­ности за их не­соб­лю­дение; * Не ис­поль­зу­ют­ся сер­ти­фици­рован­ные средс­тва за­щиты ин­форма­ции от НСД; * Не ис­поль­зу­ют­ся сер­ти­фици­рован­ные средс­тва ан­ти­вирус­ной за­щиты, ба­зы ви­рус­ных сиг­на­тур ре­гуляр­но не об­новля­ют­ся; * От­ветс­твен­ный за экс­плу­ата­цию средств крип­тогра­фичес­кой за­щиты наз­на­ча­ет­ся из чис­ла осо­бо до­верен­ных лиц |
| 1.2 | Про­веде­ние атак на эта­пе экс­плу­ата­ции СКЗИ на сле­ду­ющие объ­ек­ты: – до­кумен­та­цию на СКЗИ и ком­по­нен­ты СФ; – по­меще­ния, в ко­торых на­ходит­ся со­вокуп­ность прог­рам­мных и тех­ни­чес­ких эле­мен­тов сис­тем об­ра­бот­ки дан­ных, спо­соб­ных фун­кци­они­ровать са­мос­то­ятель­но или в сос­та­ве дру­гих сис­тем, на ко­торых ре­али­зова­ны СКЗИ и СФ | Нет | * От­ветс­твен­ный за экс­плу­ата­цию средств крип­тогра­фичес­кой за­щиты наз­на­ча­ет­ся из чис­ла осо­бо до­верен­ных лиц; * До­кумен­та­ция на СКЗИ хра­нит­ся у от­ветс­твен­но­го за экс­плу­ата­цию средств крип­тогра­фичес­кой за­щиты в ме­тал­ли­чес­ком сей­фе (шка­фу); * По­меще­ния, в ко­торых рас­по­лага­ют­ся до­кумен­та­ция на СКЗИ, СКЗИ и ком­по­нен­ты СФК, ос­на­щены вход­ны­ми дверь­ми с зам­ка­ми; * Обес­пе­чива­ет­ся пос­то­ян­ное зак­ры­тие две­рей по­меще­ний, в ко­торых рас­по­лага­ют­ся до­кумен­та­ция на СКЗИ, СКЗИ и ком­по­нен­ты СФК, на за­мок и их от­кры­тие толь­ко для сан­кци­они­рован­но­го про­хода |
| 1.3 | По­луче­ние в рам­ках пре­дос­тавлен­ных пол­но­мочий, а так­же в ре­зуль­та­те наб­лю­дений сле­ду­ющей ин­форма­ции: – све­дений о фи­зичес­ких ме­рах за­щиты объ­ек­тов, в ко­торых раз­ме­щены ре­сур­сы ин­форма­ци­он­ной сис­те­мы; – све­дений о ме­рах по обес­пе­чению кон­тро­лиру­емой зо­ны объ­ек­тов, в ко­торых раз­ме­щены ре­сур­сы ин­форма­ци­он­ной сис­те­мы; – све­дений о ме­рах по раз­гра­ниче­нию дос­ту­па в по­меще­ния, в ко­торых на­ходят­ся СВТ, на ко­торых ре­али­зова­ны СКЗИ и СФ | Нет | * Ра­бота поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов и поль­зо­вате­лей крип­тосредств рег­ла­мен­ти­рова­на; * Про­водит­ся обу­чение поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов ме­рам по за­щите ин­форма­ции и пре­дуп­режде­ние об от­ветс­твен­ности за их не­соб­лю­дение; * Све­дения о фи­зичес­ких ме­рах за­щиты объ­ек­тов, в ко­торых раз­ме­щена ГИС в сфе­ре фи­нан­сов, дос­тупны ог­ра­ничен­но­му кру­гу сот­рудни­ков |
| 1.4 | Ис­поль­зо­вание штат­ных средств ИС, ог­ра­ничен­ное ме­рами, ре­али­зован­ны­ми в ин­форма­ци­он­ной сис­те­ме, в ко­торой ис­поль­зу­ет­ся СКЗИ, и нап­равлен­ны­ми на пре­дот­вра­щение и пре­сече­ние не­сан­кци­они­рован­ных дей­ствий | Да | * Ра­бота поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов и поль­зо­вате­лей крип­тосредств рег­ла­мен­ти­рова­на; * От­ветс­твен­ный за за­щиту ин­форма­ции, ад­ми­нис­тра­торы ГИС в сфе­ре фи­нан­сов наз­на­ча­ют­ся из чис­ла осо­бо до­верен­ных лиц; * Ре­монт, об­слу­жива­ние и соп­ро­вож­де­ние прог­рам­мных, тех­ни­чес­ких и прог­рам­мно-тех­ни­чес­ких средств ГИС в сфе­ре фи­нан­сов, в том чис­ле СЗИ, вы­пол­ня­ет­ся до­верен­ны­ми ли­цами, с вы­пол­не­ни­ем мер по за­щите ин­форма­ции; * Про­водит­ся обу­чение поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов ме­рам по за­щите ин­форма­ции и пре­дуп­режде­ние об от­ветс­твен­ности за их не­соб­лю­дение; * Не ис­поль­зу­ют­ся сер­ти­фици­рован­ные средс­тва за­щиты ин­форма­ции от НСД; * Не ис­поль­зу­ют­ся сер­ти­фици­рован­ные средс­тва ан­ти­вирус­ной за­щиты, ба­зы ви­рус­ных сиг­на­тур ре­гуляр­но не об­новля­ют­ся; * Поль­зо­вате­ли ГИС в сфе­ре фи­нан­сов не име­ют воз­можнос­ти за­пус­ка сто­рон­не­го или ус­та­нов­ки, из­ме­нения нас­тро­ек име­юще­гося прог­рам­мно­го обес­пе­чения без кон­тро­ля со сто­роны от­ветс­твен­но­го за за­щиту ин­форма­ции; * Прог­рам­мные, тех­ни­чес­кие, прог­рам­мно-тех­ни­чес­кие средс­тва, в том чис­ле и СЗИ, нас­тро­ены до­верен­ны­ми ли­цами и со­от­ветс­тву­ют тре­бова­ни­ям по за­щите ин­форма­ции |
| 2.1 | Фи­зичес­кий дос­туп к СВТ, на ко­торых ре­али­зова­ны СКЗИ и СФ | Нет | * Об­слу­жива­ющий пер­со­нал и ли­ца, обес­пе­чива­ющие фун­кци­они­рова­ние ГИС в сфе­ре фи­нан­сов, не име­ют воз­можнос­ти на­ходить­ся в по­меще­ни­ях, где рас­по­ложе­на ГИС в сфе­ре фи­нан­сов, в от­сутс­твие поль­зо­вате­лей ГИС в сфе­ре фи­нан­сов; * В по­меще­ни­ях, в ко­торых про­ис­хо­дит об­ра­бот­ка за­щища­емой ин­форма­ции, не­воз­можно на­хож­де­ние пос­то­рон­них лиц; * По­меще­ния, в ко­торых рас­по­лага­ют­ся до­кумен­та­ция на СКЗИ, СКЗИ и ком­по­нен­ты СФК, ос­на­щены вход­ны­ми дверь­ми с зам­ка­ми; * Обес­пе­чива­ет­ся пос­то­ян­ное зак­ры­тие две­рей по­меще­ний, в ко­торых рас­по­лага­ют­ся до­кумен­та­ция на СКЗИ, СКЗИ и ком­по­нен­ты СФК, на за­мок и их от­кры­тие толь­ко для сан­кци­они­рован­но­го про­хода |
| 2.2 | Воз­можность воз­дей­ство­вать на ап­па­рат­ные ком­по­нен­ты СКЗИ и СФ, ог­ра­ничен­ная ме­рами, ре­али­зован­ны­ми в ин­форма­ци­он­ной сис­те­ме, в ко­торой ис­поль­зу­ет­ся СКЗИ, и нап­равлен­ны­ми на пре­дот­вра­щение и пре­сече­ние не­сан­кци­они­рован­ных дей­ствий | Нет | * В по­меще­ни­ях, в ко­торых про­ис­хо­дит об­ра­бот­ка за­щища­емой ин­форма­ции, не­воз­можно на­хож­де­ние пос­то­рон­них лиц; * По­меще­ния, в ко­торых рас­по­лага­ют­ся до­кумен­та­ция на СКЗИ, СКЗИ и ком­по­нен­ты СФК, ос­на­щены вход­ны­ми дверь­ми с зам­ка­ми; * Обес­пе­чива­ет­ся пос­то­ян­ное зак­ры­тие две­рей по­меще­ний, в ко­торых рас­по­лага­ют­ся до­кумен­та­ция на СКЗИ, СКЗИ и ком­по­нен­ты СФК, на за­мок и их от­кры­тие толь­ко для сан­кци­они­рован­но­го про­хода; * Кор­пу­са сис­темных бло­ков за­щище­ны от вскры­тия (опе­чата­ны/оп­ломби­рова­ны) |
| 3.1 | Соз­да­ние спо­собов, под­го­тов­ка и про­веде­ние атак с прив­ле­чени­ем спе­ци­алис­тов в об­ласти ана­лиза сиг­на­лов, соп­ро­вож­да­ющих фун­кци­они­рова­ние СКЗИ и СФ, и в об­ласти ис­поль­зо­вания для ре­али­зации атак не­доку­мен­ти­рован­ных (не­дек­ла­риро­ван­ных) воз­можнос­тей прик­ладно­го ПО | Нет | Не осу­щест­вля­ет­ся об­ра­бот­ка све­дений, сос­тавля­ющих го­сударс­твен­ную тай­ну, а так­же иных све­дений, ко­торые мо­гут пред­став­лять ин­те­рес для ре­али­зации воз­можнос­ти. Вы­сокая сто­имость и слож­ность под­го­тов­ки ре­али­зации воз­можнос­ти |
| 3.2 | Про­веде­ние ла­бора­тор­ных ис­сле­дова­ний СКЗИ, ис­поль­зу­емых вне кон­тро­лиру­емой зо­ны, ог­ра­ничен­ное ме­рами, ре­али­зован­ны­ми в ин­форма­ци­он­ной сис­те­ме, в ко­торой ис­поль­зу­ет­ся СКЗИ, и нап­равлен­ны­ми на пре­дот­вра­щение и пре­сече­ние не­сан­кци­они­рован­ных дей­ствий | Нет | Не осу­щест­вля­ет­ся об­ра­бот­ка све­дений, сос­тавля­ющих го­сударс­твен­ную тай­ну, а так­же иных све­дений, ко­торые мо­гут пред­став­лять ин­те­рес для ре­али­зации воз­можнос­ти. Вы­сокая сто­имость и слож­ность под­го­тов­ки ре­али­зации воз­можнос­ти |
| 3.3 | Про­веде­ние ра­бот по соз­да­нию спо­собов и средств атак в на­уч­но-ис­сле­дова­тель­ских цен­трах, спе­ци­али­зиру­ющих­ся в об­ласти раз­ра­бот­ки и ана­лиза СКЗИ и СФ, в том чис­ле с ис­поль­зо­вани­ем ис­ходных тек­стов вхо­дяще­го в СФ прик­ладно­го ПО, не­пос­редс­твен­но ис­поль­зу­юще­го вы­зовы прог­рам­мных фун­кций СКЗИ | Нет | Не осу­щест­вля­ет­ся об­ра­бот­ка све­дений, сос­тавля­ющих го­сударс­твен­ную тай­ну, а так­же иных све­дений, ко­торые мо­гут пред­став­лять ин­те­рес для ре­али­зации воз­можнос­ти. Вы­сокая сто­имость и слож­ность под­го­тов­ки ре­али­зации воз­можнос­ти |
| 4.1 | Соз­да­ние спо­собов, под­го­тов­ка и про­веде­ние атак с прив­ле­чени­ем спе­ци­алис­тов в об­ласти ис­поль­зо­вания для ре­али­зации атак не­доку­мен­ти­рован­ных (не­дек­ла­риро­ван­ных) воз­можнос­тей сис­темно­го ПО | Нет | Не осу­щест­вля­ет­ся об­ра­бот­ка све­дений, сос­тавля­ющих го­сударс­твен­ную тай­ну, а так­же иных све­дений, ко­торые мо­гут пред­став­лять ин­те­рес для ре­али­зации воз­можнос­ти. Вы­сокая сто­имость и слож­ность под­го­тов­ки ре­али­зации воз­можнос­ти |
| 4.2 | Воз­можность рас­по­лагать све­дени­ями, со­дер­жа­щими­ся в конс­трук­тор­ской до­кумен­та­ции на ап­па­рат­ные и прог­рам­мные ком­по­нен­ты СФ | Нет | Не осу­щест­вля­ет­ся об­ра­бот­ка све­дений, сос­тавля­ющих го­сударс­твен­ную тай­ну, а так­же иных све­дений, ко­торые мо­гут пред­став­лять ин­те­рес для ре­али­зации воз­можнос­ти |
| 4.3 | Воз­можность воз­дей­ство­вать на лю­бые ком­по­нен­ты СКЗИ и СФ | Нет | Не осу­щест­вля­ет­ся об­ра­бот­ка све­дений, сос­тавля­ющих го­сударс­твен­ную тай­ну, а так­же иных све­дений, ко­торые мо­гут пред­став­лять ин­те­рес для ре­али­зации воз­можнос­ти |