Модель угроз безопасности информации

1. Общие положения.

2. Описание информационной системы и особенностей ее функционирования.

2.1. Цель и задачи, решаемые информационной системой.

2.2. Описание структурно-функциональных характеристик информационной системы.

2.3. Описание технологии обработки информации.

3. Возможности нарушителей (модель нарушителя).

3.1. Типы и виды нарушителей.

3.2. Возможные цели и потенциал нарушителей.

3.3. Возможные способы реализации угроз безопасности информации.

4. Актуальные угрозы безопасности информации.

Приложения (при необходимости).

**1. Общие положения.**

***Примечание*:** *Раздел «Общие положения» содержит назначение и область действия документа, информацию о полном наименовании информационной системы, для которой разработана модель угроз безопасности информации, а также информацию об использованных для разработки модели угроз безопасности информации нормативных и методических документах, национальных стандартах. В данный раздел также включается информация об используемых данных и источниках, на основе которых определяются угрозы безопасности информации (документация, исходные тексты программ, опросы персонала, журналы регистрации средств защиты, отчеты об аудите и иные источники).*

Настоящая модель угроз безопасности информации (далее – Модель) разработана для [*ПОЛНОЕ НАИМЕНОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ*] (далее – ИС), и содержит систематизированный перечень угроз безопасности информации, обрабатываемой с использованием технологий виртуализации аппаратного обеспечения.

Для составления Модели использовались следующие источники:

* Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России (http://bdu.fstec.ru/threat)
* Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России (http://bdu.fstec.ru/threat)
* Методика определения угроз безопасности информации в информационных системах (проект) http://fstec.ru/component/attachments/download/812
* Проект ГОСТ Р Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения.

В приложении к настоящей модели представлены меры защиты информации, изложенные в настоящем стандарте, предназначены для применения только в случае обработки информации с использованием технологий виртуализации.

**2. Описание информационной системы и особенностей ее функционирования.**

***Примечание*:** *Раздел* *«Описание информационной системы и особенностей ее функционирования» содержит общую характеристику информационной системы, описание структурно-функциональных характеристик информационной системы, описание взаимосвязей между сегментами информационной системы, описание взаимосвязей с другими информационными системами и информационно-телекоммуникационными сетями, описание технологии обработки информации. Также в данном разделе приводятся предположения, касающиеся информационной системы и особенностей ее функционирования (в частности предположения об отсутствии неучтенных беспроводных каналов доступа или динамичность выделения адресов узлам информационной системы, иные предположения). В раздел включаются любые ограничения, касающиеся информационной системы и особенностей ее функционирования.*

2.1. Цель и задачи, решаемые информационной системой.

2.2. Описание структурно-функциональных характеристик информационной системы.

2.3. Описание технологии обработки информации.

Вариант 1

ИС представляет собой тестовую среду Организации и предназначена для:

Проведения предварительного тестирования программного обеспечения, планируемого для внедрения в Организации.

для запуска ПО в среде операционной системы, которая его не поддерживает;

для запуска нескольких операционных систем (в том числе, различных) на одном физическом компьютере;

для создания и восстановление состояния компьютеров, входящих в состав ИС.

Вариант 2

ИС предназначена для решения задач управления персоналом и реализации уставных целей. Объекты ИС размещаются на территории г. \_\_\_\_\_\_\_\_\_. В составе ИС функционирует 5 АРМ и 10 виртуальных серверов. Рассматриваемая ИС имеет подключение к сетям общего пользования и международного обмена. Все компоненты ИС находятся на одном объекте, внутри контролируемой зоны. Обработка информации данных ведется в многопользовательском режиме, без ограничения прав доступа. Все технические средства находятся в пределах РБ. К информации данным предъявляются требования целостности и доступности.

При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИС. Все пользователи имеют собственные роли: администратор безопасности, пользователи с правом чтения-записи, пользователи с правом чтения данных.

Виртуализация аппаратного обеспечения применяется в ИС для:

для запуска ПО в среде операционной системы, которая его не поддерживает;

для запуска нескольких операционных систем (в том числе, различных) на одном физическом компьютере;

для создания и восстановление состояния компьютеров, входящих в состав ИС.

Уровень проектной защищенности ИС – Низкий

Под уровнем проектной защищенности понимается исходная защищенность ИС, обусловленная заданными при проектировании структурно-функциональными характеристиками и условиями ее функционирования.

Уровень проектной защищенности определяется на основе анализа проектных структурно-функциональных характеристик, приведенных в таблице ниже.

Показатели, характеризующие проектную защищенность информационной системы

|  |  |  |  |
| --- | --- | --- | --- |
| Структурно-функциональные характеристики информационной системы, условия ее эксплуатации | Уровень проектной защищенности информационной системы | | |
| Высокий | Средний | Низкий |
| **1. По структуре информационной системы:** |  |  |  |
| * автономное автоматизированное рабочее место; | ✓ |  |  |
| * локальная информационная система; |  | ✓ |  |
| * распределенная информационная система. |  |  | ✓ |
| **2. По используемым информационным технологиям:** |  |  |  |
| * системы на основе виртуализации; |  |  | ✓ |
| * системы, реализующие «облачные вычисления»; |  |  | ✓ |
| * системы с мобильными устройствами; |  |  | ✓ |
| * системы с технологиями беспроводного доступа; |  |  | ✓ |
| * грид-системы; |  |  | ✓ |
| * суперкомпьютерные системы. |  | ✓ |  |
| **3. По архитектуре информационной системы:** |  |  |  |
| * системы на основе «тонкого клиента»; | ✓ |  |  |
| * системы на основе одноранговой сети; |  | ✓ |  |
| * файл-серверные системы; |  |  | ✓ |
| * центры обработки данных; |  |  | ✓ |
| * системы с удаленным доступом пользователей; |  |  | ✓ |
| * использование разных типов операционных систем (гетерогенность среды); |  | ✓ |  |
| * использование прикладных программ, независимых от операционных систем; |  | ✓ |  |
| * использование выделенных каналов связи. |  | ✓ |  |
| **4. По наличию (отсутствию) взаимосвязей с иными информационными системами:** |  |  |  |
| * взаимодействующая с системами; |  |  | ✓ |
| * невзаимодействующая с системами. |  | ✓ |  |
| **5. По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования:** |  |  |  |
| * подключенная; |  |  | ✓ |
| * подключенная через выделенную инфраструктуру; |  | ✓ |  |
| * неподключенная. | ✓ |  |  |
| **6. По размещению технических средств:** |  |  |  |
| * расположенные в пределах одной контролируемой зоны; | ✓ |  |  |
| * расположенные в пределах нескольких контролируемых зон; |  | ✓ |  |
| * расположенные вне контролируемой зоны. |  |  | ✓ |
| **7. По режимам обработки информации в информационной системе:** |  |  |  |
| * многопользовательский; |  |  | ✓ |
| * однопользовательский. | ✓ |  |  |
| **8. По режимам разграничения прав доступа:** |  |  |  |
| * без разграничения; |  |  | ✓ |
| * с разграничением. |  | ✓ |  |
| **9. По режимам разделения функций по управлению информационной системой:** |  |  |  |
| * без разделения; |  |  | ✓ |
| * выделение рабочих мест для администрирования в отдельный домен; |  | ✓ |  |
| * использование различных сетевых адресов; |  | ✓ |  |
| * использование выделенных каналов для администрирования. |  | ✓ |  |
| **10. По подходам к сегментированию информационной системы:** |  |  |  |
| * без сегментирования; |  |  | ✓ |
| * с сегментированием. |  | ✓ |  |
| **ИТОГО:** |  |  |  |

В ходе создания информационной системы уровень ее проектной защищенности определяется следующим образом:

* а) информационная система имеет **высокий** уровень проектной защищенности, если не менее 80% характеристик информационной системы соответствуют уровню «высокий» (суммируются положительные решения по второму столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по третьему столбцу);
* б) информационная система имеет **средний** уровень проектной защищенности, если не выполняются условия по пункту а) и не менее 90% характеристик информационной системы соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по третьему столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности;
* в) информационная система имеет **низкий** уровень проектной защищенности, если не выполняются условия по пунктам а) и б).

Матрица требований, предъявляемых к защищаемым активам

|  |  |  |  |
| --- | --- | --- | --- |
| **Объект защиты** | Конфиденциальность | Целостность | Доступность |
| Виртуальная машина | ✓ | ✓ | ✓ |
| Образ виртуальной машины | ✓ | ✓ | ✓ |
| Гипервизор | ✓ | ✓ | ✓ |
| Консоль управления гипервизором | ✓ | ✓ | ✓ |
| Виртуальные устройства | ✓ | ✓ | ✓ |
| Виртуальные устройства хранения, обработки и передачи данных | ✓ | ✓ | ✓ |
| Виртуальные устройства хранения данных | ✓ | ✓ | ✓ |
| Виртуальные диски | ✓ | ✓ | ✓ |

К основным объектам, подлежащим защите от НСД, относятся:

* объекты файловой системы виртуальных и физических дисков, данные на машинных носителях информации (файлы-образы, файлы, содержащие настройки виртуализированного ПО, хранимая информация конфиденциального характера и др.);
* гипервизоры (гипервизор I типа, гипервизор II типа, гипервизор системы хранения данных и др.);
* системные и прикладные программы (службы, сервисы, драйверы и др.);
* служебная информация системных и прикладных программ (параметры запуска, параметры установки, параметры конфигурации и др.);
* средства ЗИ (средства идентификации и аутентификации, субъектов доступа и объектов доступа, средства управления доступом субъектов доступа к объектам доступа, средства контроля установки и запуска программ, средства стирания данных и остаточной информации, средства регистрации и учёта, средства криптографической защиты информации, средства антивирусной защиты, системы обнаружения (предотвращения) вторжений, средства контроля целостности, резервного копирования и восстановления, межсетевые экраны и др.);
* служебная информация средств ЗИ (параметры запуска, параметры установки, временные файлы и др.);
* процессы и потоки, запущенные в оперативной памяти (системных программ, прикладных программ, средств ЗИ, системные сервисы, драйвера, службы и др.);
* служебная информация аппаратных и виртуальных устройств обработки данных (параметры запуска, параметры установки, параметры конфигурации и др.);
* каналы передачи данных (физические/виртуальные каналы передачи (каналы связи), сетевые узлы, мобильные сетевые устройства, сетевые устройства хранения данных, устройства преобразования сетевого трафика и др.);
* активное и пассивное сетевое оборудование, его микропрограммное обеспечение (коммутаторы, сетевые карты, межсетевые экраны, кабельные сети и др.);
* служебная информация активного и пассивного сетевого оборудования (параметры запуска, параметры установки и др.);
* резервные копии данных (физического и (или) виртуального дискового пространства, используемого для хранения журналов событий гипервизора и (или) виртуальных машин, файлов-образов виртуализированного ПО и виртуальных машин, защищаемой информации в гипервизоре и (или) виртуальных машинах, защищаемой информации хранимой на физических и (или) виртуальных носителях информации и др.).

**3. Возможности нарушителей (модель нарушителя).**

***Примечание*:** *Раздел* *«Возможности нарушителей (модель нарушителя)» содержит описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации в информационной системе, способов реализации угроз безопасности информации. В данный раздел также включаются предположения, касающиеся нарушителей (в частности предположение об отсутствии у нарушителя возможности доступа к оборудованию, сделанному на заказ и применяемому при реализации угрозы, предположение о наличии (отсутствии) сговора между внешними и внутренними нарушителями или иные предположения). В раздел включаются любые ограничения, касающиеся определения нарушителей (в частности исключение администраторов информационной системы или администраторов безопасности из числа потенциальных нарушителей или иные предположения).*

3.1. Типы и виды нарушителей.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам ИС нарушители подразделяются на два типа:

* внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
* внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Угрозы безопасности информации в ИС могут быть реализованы следующими видами нарушителей:

* ~~специальные службы иностранных государств (блоков государств);~~
* ~~террористические, экстремистские группировки;~~
* преступные группы (криминальные структуры);
* внешние субъекты (физические лица);
* конкурирующие организации;
* разработчики, производители, поставщики программных, технических и программно-технических средств;
* лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ; лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);
* пользователи информационной системы;
* администраторы информационной системы и администраторы безопасности;
* бывшие работники (пользователи).

3.2. Возможные цели и потенциал нарушителей.

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

* нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
* нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
* нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №, п.п. | Вид нарушителя | Тип нарушителя | Возможные цели | Базовый потенциал | Возможности по реализации угроз безопасности информации |
| 1 | Специальные службы иностранных государств (блоков государств) | Внешний, внутренний | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций | Высокий | Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений |
| 2 | Террористические, экстремистские группировки | Внешний | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций | средний | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |
| 3 | Преступные группы (криминальные структуры) | Внешний | Причинение имущественного ущерба путем мошенничества или иным преступным путем.  Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | средний | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |
| 4 | Внешние субъекты (физические лица) | Внешний | Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | низкий | Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему |
| 5 | Конкурирующие организации | Внешний | Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием | средний | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |
| 6 | Разработчики, производители, поставщики программных, технических и программно-технических средств | Внешний | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия | средний | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |
| 7 | Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия | низкий | Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему |
| 8 | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия | низкий | Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему |
| 9 | Пользователи информационной системы | Внутренний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия | низкий | Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему. |
| 10 | Администраторы информационной системы и администраторы безопасности | Внутренний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия | средний | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |
| 11 | Бывшие работники (пользователи) | Внешний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия | низкий | Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему |

3.3. Возможные способы реализации угроз безопасности информации.

Угрозы безопасности информации могут быть реализованы нарушителями за счет:

* несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));
* несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);
* несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);
* несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);
* несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации; воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

**4. Актуальные угрозы безопасности информации.**

***Примечание*:** *Раздел* *«Актуальные угрозы безопасности информации» содержит описание актуальных угроз безопасности, включающее наименование угрозы безопасности информации, возможности нарушителя по реализации угрозы, используемые уязвимости информационной системы, описание способов реализации угрозы безопасности информации, объекты воздействия, возможные результат и последствия от реализации угрозы безопасности информации.*

Возможность реализации угрозы безопасности определяется:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень защищенности  Потенциал нарушителя | **Высокий** | **Средний** | **Низкий** |
| **Низкий** | Низкая | Средняя | Высокая |
| **Средний** | Средняя | Высокая | Высокая |
| **Высокий** | Высокая | Высокая | Высокая |

Определение степени возможного ущерба от реализации угрозы:

|  |  |
| --- | --- |
| **Степень ущерба** | **Характеристика ущерба** |
| Высокая | В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции |
| Средняя | В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций |
| Низкая | В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств |

Определение актуальности угрозы безопасности информации

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы | Степень возможного ущерба | | |
| **Низкая** | **Средняя** | **Высокая** |
| **Низкая** | Неактуальная | Неактуальная | Актуальная |
| **Средняя** | Неактуальная | Актуальная | Актуальная |
| **Высокая** | Актуальная | Актуальная | Актуальная |

При использовании виртуализации аппаратного обеспечения создаются угрозы БИ, связанные с невозможностью прямого доступа к аппаратному обеспечению со стороны ПО, использующего ресурсы виртуального аппаратного обеспечения, трудностью обеспечения полной совместимости виртуального аппаратного обеспечения с физическим аппаратным обеспечением различных фирм-производителей. К таким угрозам относятся:

* нарушение работоспособности ИС за счёт НСД к средствам виртуализации;
* атака на виртуальные каналы передачи;
* нарушение изоляции пользовательских данных внутри ВМ;
* атака на защищаемое виртуальное аппаратное обеспечение из физической сети;
* атака на защищаемое виртуальное аппаратное обеспечение из виртуальной сети;
* неконтролируемый рост числа зарезервированных вычислительных ресурсов;
* перехват управления в среде виртуализации;
* доступ к данным за пределами адресного пространства, выделенного под виртуальное аппаратное обеспечение.

**Угрозы безопасности информации (ИС построенные с использованием технологий виртуализации)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Идентификатор УБИ | Наименование УБИ | Описание | Источник угрозы (характеристика и потенциал нарушителя) | Объект воздействия | Нарушение конфиденциальности | Нарушение целостности | Нарушение доступности |
| 7 | Угроза воздействия на программы с высокими привилегиями | Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: обладания дискредитируемой программой повышенными привилегиями в системе; осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя; нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик | 1 | 1 | 0 |
| 10 | Угроза выхода процесса за пределы виртуальной машины | Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки виртуализации на уровне процессора. Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Информационная система, сетевой узел, носитель информации, объекты файловой системы, учётные данные пользователя, образ виртуальной машины | 1 | 1 | 1 |
| 20 | Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг | Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг | Внутренний нарушитель с низким потенциалом | Облачная система, виртуальная машина | 1 | 1 | 1 |
| 23 | Угроза изменения компонентов системы | Угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах файлах, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе. Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации информационной системы. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе | Внутренний нарушитель с низким потенциалом | Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение | 0 | 1 | 1 |
| 27 | Угроза искажения вводимой и выводимой на периферийные устройства информации | Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок | Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом | Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение | 0 | 1 | 0 |
| 44 | Угроза нарушения изоляции пользовательских данных внутри виртуальной машины | Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Виртуальная машина, гипервизор | 1 | 1 | 1 |
| 46 | Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия. Данная угроза обусловлена наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между её уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия | Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом | Сетевой узел, сетевое программное обеспечение, метаданные, учётные данные пользователя | 1 | 0 | 1 |
| 48 | Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин | Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов; к нарушению целостности программ, установленных на виртуальных машинах; к нарушению доступности ресурсов виртуальных машин; к созданию ботнета путём внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы) | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина | 1 | 1 | 1 |
| 52 | Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения | Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях. Также данная угроза обуславливает ограничение возможности смены производителей аппаратного и программного обеспечения поставщиком облачных услуг, что может привести к нарушению целостности и доступности информации по вине поставщика облачных услуг | Внешний нарушитель с низким потенциалом | Облачная инфраструктура, виртуальная машина, аппаратное обеспечение, системное программное обеспечение | 0 | 1 | 1 |
| 58 | Угроза неконтролируемого роста числа виртуальных машин | Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин. Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания виртуальных машин. Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре | Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом | Облачная система, консоль управления облачной инфраструктурой, облачная инфраструктура | 0 | 0 | 1 |
| 59 | Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов | Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Данная угроза обусловлена уязвимостями программного обеспечения уровня управления виртуальной инфраструктурой, реализующего функцию распределения компьютерных ресурсов между пользователями. Реализация данной угрозы возможна при условии успешного осуществления нарушителем несанкционированного доступа к программному обеспечению уровня управления виртуальной инфраструктурой, реализующему функцию распределения компьютерных ресурсов между пользователями | Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом | Информационная система, сервер | 0 | 0 | 1 |
| 73 | Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства | 1 | 1 | 1 |
| 75 | Угроза несанкционированного доступа к виртуальным каналам передачи | Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации | Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом | Сетевое программное обеспечение, сетевой трафик, виртуальные устройства | 1 | 0 | 0 |
| 76 | Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети. Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данной угрозы возможна в одном из следующих случаев: наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Гипервизор | 0 | 0 | 1 |
| 77 | Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение | Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки. Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Сервер, рабочая станция, виртуальная машина, гипервизор, машинный носитель информации, метаданные | 0 | 1 | 1 |
| 78 | Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети | Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия | Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом | Виртуальная машина | 1 | 1 | 1 |
| 79 | Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин | Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин c помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для различные механизмы обмена данными между виртуальными машинами, реализованные в гипервизоре и активированные в системе | Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом | Виртуальная машина | 1 | 1 | 1 |
| 80 | Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети | Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Виртуальные устройства хранения, обработки и передачи данных | 1 | 1 | 1 |
| 84 | Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети | Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных). Данная угроза обусловлена наличием слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и (или) виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны с высокой сложностью алгоритмов обеспечения согласованности действий по распределению информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства. Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабостей технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.) | Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом | Виртуальные устройства хранения данных, виртуальные диски | 1 | 1 | 1 |
| 85 | Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации | Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределённых файлах, содержащих защищаемую информацию, путём восстановления данных распределённых файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределённой информации. Данная угроза обусловлена тем, что в связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Реализация данной угрозы возможна при условии недостаточности или отсутствия мер по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Носитель информации, объекты файловой системы | 1 | 0 | 0 |
| 108 | Угроза ошибки обновления гипервизора | Угроза заключается в возможности дискредитации нарушителем функционирующих на базе гипервизора защитных механизмов, предотвращающих несанкционированный доступ к образам виртуальных машин, из-за ошибок его обновления. Данная угроза обусловлена зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или её части, если используется более одного гипервизора) от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: сбоев в процессе его обновления; обновлений, в ходе которых внедряются новые ошибки в код гипервизора; обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования; других инцидентов безопасности информации | Внутренний нарушитель с низким потенциалом | Системное программное обеспечение, гипервизор | 1 | 1 | 1 |
| 119 | Угроза перехвата управления гипервизором | Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счёт получения нарушителем права управления гипервизором путём эксплуатации уязвимостей консоли управления гипервизором. Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Системное программное обеспечение, гипервизор, консоль управления гипервизором | 1 | 1 | 1 |
| 120 | Угроза перехвата управления средой виртуализации | Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым всеми гипервизорами, реализующими среду виртуализации, за счёт получения нарушителем права управления этими гипервизорами путём эксплуатации уязвимостей консоли средства управления виртуальной инфраструктурой. Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой | Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом | Информационная система, системное программное обеспечение | 1 | 1 | 1 |

**Угрозы безопасности информации (ИС построенные с использованием технологий облачных вычислений)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Идентификатор УБИ | Наименование УБИ | Описание | Источник угрозы (характеристика и потенциал нарушителя) | Объект воздействия | Нарушение конфиденциальности | Нарушение целостности | Нарушение доступности |
| 20 | Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг | Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг | Внутренний нарушитель с низким потенциалом | Облачная система, виртуальная машина | 1 | 1 | 1 |
| 21 | Угроза злоупотребления доверием потребителей облачных услуг | Угроза заключается в возможности нарушения (случайно или намеренно) защищённости информации потребителей облачных услуг внутренними нарушителями поставщика облачных услуг. Данная угроза обусловлена тем, что значительная часть функций безопасности переведена в сферу ответственности поставщика облачных услуг, а также невозможностью принятия потребителем облачных услуг мер защиты от действий сотрудников поставщика облачных услуг. Реализация данной угрозы возможна при условии того, что потребители облачных услуг не входят в состав организации, осуществляющей оказание данных облачных услуг (т.е. потребитель действительно передал поставщику собственную информацию для осуществления её обработки) | Внешний нарушитель с низким потенциалом | Облачная система | 1 | 1 | 0 |
| 27 | Угроза искажения вводимой и выводимой на периферийные устройства информации | Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок | Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом | Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение | 0 | 1 | 0 |

**Приложения (при необходимости).**

Меры защиты информации

Обеспечение (поддержание) БИ при использовании виртуализации аппаратного обеспечения требует обеспечения защиты виртуального аппаратного обеспечения, ПО, реализующего такой тип виртуализации, а также защиту самого аппаратного обеспечения, в отношении которого проводится виртуализация. Мерами защиты информации при использовании виртуализации аппаратного обеспечения являются:

* разделение физических ресурсов между компонентами виртуальной инфраструктуры в зависимости от уровня конфиденциальности обрабатываемой информации;
* контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;
* стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуализированного ПО и виртуального аппаратного обеспечения;
* учёт изменений в составе и конфигурации аппаратной части ИС во время её функционирования и в период её аппаратного отключения;
* учёт запуска (завершения) работы компонентов виртуальной инфраструктуры;
* регистрация изменений состава и конфигурации виртуального аппаратного обеспечения;
* регистрация изменений правил доступа к виртуальному аппаратному обеспечению;
* регистрация изменений прав доступа к файлам-образам виртуализированного ПО и виртуальных машин, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;
* размещение сенсоров и (или) датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;
* контроль целостности микропрограммного обеспечения аппаратной части ИС;
* контроль работоспособности дублирующих ключевых компонентов аппаратного обеспечения ИС;
* резервное копирование защищаемой информации, , хранимой на физических носителях информации;
* своевременное обнаружение отказов компонентов виртуальной инфраструктуры;
* мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;
* контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры;
* предотвращение задержки или прерывания выполнения в виртуальной инфраструктуре процессов с высоким приоритетом со стороны процессов с низким приоритетом;
* обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами ЗИ (функциями безопасности средств ЗИ);
* передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией конфиденциального характера, обрабатываемой в виртуальной инфраструктуре, при обмене информацией с иными ИС;
* выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешённых сетевых протоколов;
* создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз БИ;
* воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик физических или виртуальных сегментов ИС, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках ИС.