Перечень анализируемых угроз безопасности информации

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
1	Угрозы доступа в операционную среду				
1.1	Угрозы, реализуемые в ходе загрузки ОС				
1.1.1	32	Угроза использования поддельных цифровых подписей BIOS/ Ц	Угроза заключается в возможности установки уязвимой версии обновления BIOS/UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер по контролю за благонадежностью центров выдачи цифровых подписей. Реализация данной угрозы возможна при условии выдачи неблагонадежным центром сертификации цифровой подписи на версию обновления BIOS/UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений	Внешний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
1.1.2	35	Угроза использования слабых криптографических алгоритмов BIOS/ КДЦ	Угроза заключается в сложности проверки реальных параметров работы и алгоритмов, реализованных в криптографических средствах BIOS/UEFI. При этом доверие к криптографической защите будет ограничено доверием к производителю BIOS. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI. Возможность реализации данной угрозы снижает	Внешний нарушитель с высоким потенциалом	Микропрограммное обеспечение BIOS/UEFI

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			достоверность оценки реального уровня защищённости системы		
1.1.3	39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS/ Ц	Угроза заключается в возможности нарушения (невозможности осуществления) процедуры обновления BIOS/UEFI при исчерпании запаса необходимых для ее проведения ключей. Данная угроза обусловлена ограниченностью набора ключей, необходимых для обновления BIOS/UEFI. Реализация данной угрозы возможна путем эксплуатации уязвимостей средств обновления набора ключей, или путем использования нарушителем программных средств перебора ключей	Внешний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI
1.1.4	87	Угроза несанкционированного использования привилегированных функций BIOS/ КДЦ	Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI
1.1.5	127	Угроза подмены действия пользователя путем обмана/ КДЦ	Угроза заключается в возможности нарушителя выполнения неправомерных действий в системе от имени другого пользователя с помощью методов социальной инженерии (обмана пользователя, навязывание ложных убеждений) или технических методов (использование прозрачных кнопок, подмена надписей на элементах управления и др.).	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			Данная угроза обусловлена слабостями интерфейса взаимодействия с пользователем или ошибками пользователя. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя прав на проведение нужных от него нарушителю операций		
1.1.6	150	Угроза сбоя процесса обновления BIOS/ Д	Угроза заключается в возможности выведения из строя компьютера из-за внесения критических ошибок в программное обеспечение BIOS/UEFI в результате нарушения процесса его обновления. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера как при установке корректной/совместимой версии обновления (из-за сбоев, помех и т.п.), так и при установке поврежденной/несовместимой версии обновления (из-за отсутствия механизма проверки целостности и совместимости)	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи
1.1.7	154	Угроза установки уязвимых версий обновления программного обеспечения BIOS/ КДЦ	Угроза заключается в возможности внесения уязвимостей в программное обеспечение BIOS/UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации BIOS/UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями мер контроля	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера		
1.1.8	213	Угроза обхода многофакторной аутентификации	Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты, участвующие в процедуре многофакторной аутентификации. Данная угроза обусловлена: наличием уязвимостей программного обеспечения; слабостями мер антивирусной защиты и разграничения доступа. Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; при наличии у него привилегий установки программного обеспечения	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя
1.2	Угрозы, реализуемые после загрузки ОС				
1.2.1	7	Угроза воздействия на программы с высокими привилегиями/ КЦ	Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путем использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер разграничения доступа.	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			Реализация данной угрозы возможна при условиях: обладания дискредитируемой программой повышенными привилегиями в системе; осуществления дискредитируемой программой приема входных данных от других программ или от пользователя; нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе		
1.2.2	16	Угроза доступа к локальным файлам сервера при помощи URL/ К	Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделен при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение
1.2.3	25	Угроза изменения системных и глобальных переменных/ КДЦ	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путем изменения используемых дискредитируемыми программами единых системных и глобальных переменных. Данная угроза обусловлена слабостями механизма контроля	Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение,

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к системным и глобальным переменным и отсутствии проверки целостности их значений со стороны дискредитируемого приложения		сетевое программное обеспечение
1.2.4	30	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию/ КДЦ	Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе, полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учетной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учетные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			об идентификационной и аутентификационной информации, соответствующей учетной записи «по умолчанию» для объекта защиты; успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты		
1.2.5	37	Угроза исследования приложения через отчеты об ошибках/ К	Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путем анализа генерируемых этим приложением отчетов об ошибках. Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчетах об ошибках. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчетам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
1.2.6	68	Угроза неправомерного/ некорректного использования интерфейса взаимодействия с приложением/ КДЦ	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). Данная угроза обусловлена наличием слабостей в механизме проверки входных данных и команд API, используемого программным обеспечением. Реализация данной угрозы возможна в условиях наличия у нарушителя доступа к API и отсутствия у дискредитируемого приложения механизма проверки вводимых данных и команд	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр
1.2.7	95	Угроза несанкционированного управления указателями/ КДЦ	Угроза заключается в возможности выполнения нарушителем произвольного вредоносного кода от имени дискредитируемого приложения или приведения дискредитируемого приложения в состояние «отказ в обслуживании» путем изменения указателей на ячейки памяти, содержащие определенные данные, используемые дискредитируемым приложением. Данная угроза связана с уязвимостями в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение указателей, используемых дискредитируемым приложением	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
1.2.8	109	Угроза перебора всех настроек и параметров приложения/ ДЦ	Угроза заключается в возможности получения нарушителем доступа к дополнительному скрытому функционалу (информация о котором не была опубликована разработчиком) или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путем перебора всех возможных комбинаций. Данная угроза обусловлена уязвимостями программного обеспечения, проявляющимися при его неправильной конфигурации. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение конфигурации программного обеспечения. При реализации данной угрозы, в отличие от других подобных угроз, нарушитель действует «вслепую» простым путем перебора всевозможных комбинаций	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр
1.2.9	122	Угроза повышения привилегий/ КДЦ	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) от его (ее) имени путем эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации). Реализация данной угрозы возможна при наличии	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение, информационная система

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			у нарушителя программного обеспечения (типа «эксплойт»), специально разработанного для реализации данной угрозы в дискредитируемой системе		
1.2.10	188	Угроза подмены программного обеспечения/ КДЦ	Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счет загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. Данная угроза обусловлена наличием у пользователя прав для установки программного обеспечения из сети Интернет. Реализация данной угрозы возможна при скачивании программного обеспечения из сети Интернет	Внутренний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение
1.2.11	189	Угроза маскирования действий вредоносного кода/ ДЦ	Угроза заключается в возможности сокрытия в системе действий вредоносного кода за счет применения специальных механизмов маскирования кода (архивирование, изменение формата данных и др.), которые препятствуют его дальнейшему анализу. Данная угроза обусловлена наличием способов маскирования программного кода, не учтенных сигнатурными базами средств защиты информации, а также механизмов операционной системы, позволяющих осуществить поиск модулей средств защиты информации. Реализация данной угрозы возможна при условии использования в системе устаревших версий средств защиты информации	Внешний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
1.2.12	208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники/ Д	Угроза заключается в возможности использования вычислительных ресурсов средств вычислительной техники для осуществления сторонних вычислительных процессов. Угроза реализуется за счет внедрения в средства вычислительной техники вредоносной программы, содержащей код, реализующий использования вычислительных ресурсов для своих нужд (в частности, для майнинга криптовалюты). Данная угроза обусловлена недостаточностью следующих мер защиты информации: мер по антивирусной защите, что позволяет выполнить установку и запуск вредоносной программы; мер по ограничению программной среды, что позволяют нарушителю осуществлять бесконтрольный запуск программных компонентов	Внутренний нарушитель с низким потенциалом Внутренний нарушитель со средним потенциалом Внешний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом	Средство вычислительной техники, мобильное устройство
1.2.13	215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов/ КДЦ	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемую систему с использованием сторонних легитимных сервисов (социальных сетей, мессенджеров, репозиториев кода и т.п.), используемых в качестве посредника. Реализация данной угрозы возможна если дискредитируемая система уже скомпрометирована	Внешний нарушитель со средним потенциалом	Программное обеспечение (программы)
2	Угрозы создания нештатных режимов работы программных и программно-аппаратных средств				

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
2.1	33	Угроза использования слабостей кодирования входных данных/ ДЦ	Угроза заключается в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путем манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.). Данная угроза обусловлена слабостями механизма контроля входных данных. Реализация данной угрозы возможна при условиях: дискредитируемая система принимает входные данные от нарушителя; нарушитель обладает возможностью управления одним или несколькими параметрами входных данных	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр
2.2	61	Угроза некорректного задания структуры данных транзакции/ ДЦ	Угроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путем прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя ее ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное проведение транзакции. Данная угроза обусловлена слабостями механизма контроля непрерывности транзакций и целостности данных, передаваемых в ходе транзакции между базой данных и ее клиентом	Внутренний нарушитель со средним потенциалом	Сетевой трафик, база данных, сетевое программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
2.3	114	Угроза переполнения целочисленных переменных/ КДЦ	Угроза заключается в возможности приведения нарушителем дискредитируемого приложения к сбоям в работе путем подачи на его входные интерфейсы данных неподдерживаемого формата или выполнения с его помощью операции, в результате которой будут получены данные неподдерживаемого дискредитируемым приложением формата. Данная угроза обусловлена уязвимостями программного обеспечения, связанными с недостаточной проверкой такими приложениями корректности входных данных, а также тем, что операторы любого программного обеспечения способны правильно обрабатывать только определенные типы данных (например, только целые или только положительные числа). Реализация данной угрозы возможна при условии наличия у нарушителя: сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных; возможности взаимодействия с входным интерфейсом дискредитируемого приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
2.4	118	Угроза перехвата привилегированного процесса/ КДЦ	Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы),	Внешний нарушитель со средним потенциалом, Внутренний	Системное программное обеспечение, прикладное программное

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			для выполнения произвольного вредоносного кода с правами дискредитированного процесса. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации), приводящими к некорректному распределению прав доступа внутри древа наследуемых процессов. Реализация данной угрозы возможна при выполнении одного из условий: успешного введения нарушителем некорректных данных, приводящих к переполнению буфера или к реализации некоторых типов программных инъекций; наличия у нарушителя привилегий на запуск системных утилит, предназначенных для управления процессами	нарушитель со средним потенциалом	обеспечение, сетевое программное обеспечение
2.5	143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации/ Д	Угроза заключается в возможности прерывания нарушителем технологии обработки информации в дискредитируемой системе путем осуществления деструктивного программного (локально или удаленно) воздействия на средства хранения (внешних, съемных и внутренних накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдет в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путем простой перезагрузки системы, а потребует проведения ремонтно-восстановительных работ.	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации		
2.6	149	Угроза сбоя обработки специальным образом измененных файлов/ КДЦ	Угроза заключается в возможности осуществления нарушителем различных неправомерных действий от имени дискредитированных приложений путем вызова сбоя в их работе за счет внесения изменений в обрабатываемые дискредитируемыми программами файлы или их метаданные. Данная угроза обусловлена слабостями механизма проверки целостности обрабатываемых файлов и корректности, содержащихся в них данных. Реализация данной угрозы возможна в условиях: наличия у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке; успешно созданном в дискредитируемой системе механизме перехвата управления над обработкой нарушителем программного сбоя	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Метаданные, объекты файловой системы, системное программное обеспечение
2.7	163	Угроза перехвата исключения/сигнала	Угроза заключается в возможности нарушителя получить права на доступ к защищаемой информации путем перехвата исключений/сигналов, сгенерированных участком	Внешний нарушитель со средним	Системное программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		из привилегированного блока функций/ КДЦ	программного кода, исполняемого с повышенными привилегиями (привилегированным блоком функций) и содержащего команды по управлению защищаемой информацией. Данная угроза обусловлена тем, что вызов программных функций в привилегированном режиме подразумевает отключение для них механизмов разграничения доступа. Реализация данной угрозы возможна при следующих условиях: дискредитируемая программа, написана на языке программирования, поддерживающего механизм привилегированных блоков (например, Java); в дискредитируемой программе вызов привилегированных блоков осуществлен небезопасным способом (использовано публичное объявление внутренних функций, использована генерация исключений из привилегированного блока); нарушитель обладает правами, достаточными для перехвата программных исключений в системе	потенциалом, Внутренний нарушитель со средним потенциалом	
2.8	165	Угроза включения в проект недостоверно испытанных компонентов/ КДЦ	Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надежностью, наличием сертификатов и др. Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью.	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			Реализация данной угрозы возможна при условии выбора для применения в системе компонентов по цене, разрекламированности и др.		информационной инфраструктуры
2.9	166	Угроза внедрения системной избыточности/ Д	Угроза заключается в возможности снижения скорости обработки данных (т.е. доступности) компонентами программного обеспечения (или системы в целом) из-за внедрения в него (в нее) избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии внесения изменений в перечень задач, решаемых проектируемым программным обеспечением (проектируемой системой)	Внутренний нарушитель со средним потенциалом	Программное обеспечение, информационная система, ключевая система информационной инфраструктуры
2.10	169	Угроза наличия механизмов разработчика/ КДЦ	Угроза заключается в возможности перехвата управления программой за счет использования отладочных механизмов (специальных программных функций или аппаратных элементов, помогающих проводить тестирование и отладку средств во время их разработки). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе разработки средств защиты информации. Реализация данной угрозы возможна при условии, что в программе не удалены отладочные механизмы	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
2.11	180	Угроза отказа подсистемы обеспечения температурного режима/ Д	Угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа, входящих в нее подсистем вентиляции и температурных приборов. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путем проведения определенных мероприятий нарушителем, направленных на удаленное отключение/вывод из строя компонентов подсистемы обеспечения температурного режима	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлажденного воздуха в ЦОД, программируемые логические контроллеры, распределенные системы контроля, управленческие системы и другие программные средства контроля
2.12	195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы/ ДЦ	Угроза заключается в возможности удаленного запуска вредоносного кода за счет создания приложений, использующих обход механизмов защиты, встроенных в операционную систему. Данная угроза обусловлена ошибками в процессорах (например, ошибками в процессоре Intel поколения Haswell), позволяющими	Внешний нарушитель с высоким потенциалом	Стационарные и мобильные устройства (компьютеры и ноутбуки) (аппаратное устройство)

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			за счет создания специальных приложений осуществлять обход механизмов защиты, встроенных в операционную систему (например, механизма ASLR). Реализация данной угрозы возможна при: инициировании коллизии в таблице целевых буферов – с ее помощью можно узнать участки памяти, где находятся конкретные фрагменты кода; создании приложения, использующего эти фрагменты кода для обхода механизма защиты; запуске данного приложения в связке с эксплойтом какой-либо уязвимости самой операционной системы для создания возможности удаленного запуска вредоносного кода		
2.13	214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации/ ДЦ	Угроза заключается в пропуске и/или значительной временной задержке определения (выявления) событий безопасности информации, что приводит к отсутствию реакции на попытки несанкционированного доступа в информационную (автоматизированную) систему, на внедрение вредоносных программ. Данная угроза обусловлена некорректной настройкой компонентов информационной (автоматизированной) системы и/или средств защиты информации, а также отсутствием таких компонентов и/или средств защиты информации. Реализация данной угрозы возможна при отсутствии мер защиты, связанных с мониторингом, сбором и анализом данных о событиях информационной безопасности (отсутствием мер регистрации событий безопасности)	Внутренний нарушитель со средним потенциалом	Программное обеспечение, каналы связи (передачи) данных

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
3	Угрозы при межсетевом взаимодействии				
3.1	3	Угроза анализа криптографических алгоритмов и их реализации/ КЦ	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение
3.2	26	Угроза искажения XML-схемы/ ДЦ	Угроза заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние «отказ в обслуживании» путем изменения XML-схемы, передаваемой между клиентом и сервером. Данная угроза обусловлена слабостями мер обеспечения целостности, передаваемых при клиент-серверном взаимодействии данных, а также слабостями механизма сетевого взаимодействия открытых систем. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к сетевому трафику, передаваемому между клиентом и сервером и отсутствии	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			проверки целостности XML-схемы со стороны дискредитируемого приложения		
3.3	36	Угроза исследования механизмов работы программы/ КД	Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и дальнейшего исследования его структуры, функционала и состава в интересах определения алгоритма работы программы и поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования. Реализация данной угрозы возможна в случаях: наличия у нарушителя доступа к исходным файлам программы; наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение
3.4	102	Угроза опосредованного управления группой программ через совместно используемые данные/ ДЦ	Угроза заключается в возможности опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные, файлы конфигурации и др.). Данная угроза обусловлена наличием слабостей в механизме контроля внесенных изменений в общие данные каждой из программ в группе. Реализация данной угрозы возможна в случае успешного перехвата нарушителем управления над одной из программ в группе программ, использующих общие данные	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
3.5	131	Угроза подмены субъекта сетевого доступа/ КЦ	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путем скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника информации. Реализация данной угрозы возможна при условии успешной выдачи себя нарушителем за законного отправителя (например, с помощью ложных фишинговых веб-сайтов). Ключевое отличие от «угрозы подмены содержимого сетевых ресурсов» заключается в том, что в данном случае нарушитель не изменяет оригинального содержимого электронного ресурса (веб-сайта, электронного письма), а только служебные сведения	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик
3.6	132	Угроза получения предварительной информации об объекте защиты/ К	Угроза заключается в возможности раскрытия нарушителем защищаемых сведений о состоянии защищенности дискредитируемой системы, ее конфигурации и потенциальных уязвимостях и др. путем проведения мероприятий по сбору и анализу доступной информации о системе. Данная угроза обусловлена наличием уязвимостей в сетевом программном обеспечении, позволяющим получить сведения	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			о конфигурации отдельных программ или системы в целом (отсутствие контроля входных данных, наличие открытых сетевых портов, неправильная настройка политик безопасности и т.п.). Реализация данной угрозы возможна при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы: анализ реакций системы на сетевые (в т.ч. синтаксически неверные или нестандартные) запросы к открытым в системе сетевым сервисам, которые могут стать причиной вызова необработанных исключений с подробными сообщениями об ошибках, содержащих защищаемую информацию (о трассировке стека, о конфигурации системы, о маршруте прохождения сетевых пакетов); анализ реакций системы на строковые URI-запросы (в т.ч. неверные SQL-запросы, альтернативные пути доступа к файлам). Данная угроза отличается от угрозы перехвата данных и других угроз сбора данных тем, что нарушитель активно опрашивает дискредитируемую систему, а не просто за ней наблюдает		
3.7	212	Угроза перехвата управления информационной системой/	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам информационной системы в	Внутренний нарушитель со средним потенциалом	Инфраструктура информационных систем

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		КДЦ	результате подмены средств централизованного управления информационной системой или ее компонентами. Данная угроза обусловлена наличием у средств централизованного управления программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данным средствам централизованного управления, а также недостаточностью мер по разграничению доступа к ним. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия со средствами централизованного управления		
4	Угрозы уничтожения, хищения, модификации информации, носителей информации, аппаратных средств ИС ИАО				
4.1	27	Угроза искажения вводимой и выводимой на периферийные устройства информации/ Ц	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путем 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.	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок		
4.2	63	Угроза некорректного использования функционала программного обеспечения/ КДЦ	Угроза заключается в возможности использования декларированных возможностей программных и аппаратных средств определенным (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию. Данная угроза связана со слабостями механизма обработки данных и команд, вводимых пользователями. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к программным и аппаратным средствам	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение
4.3	111	Угроза передачи данных по скрытым каналам/ К	Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы путем ее нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путем ее маскирования под служебные протоколы, сокрытия в потоке других данных (стеганография) и т.п.	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация данной угрозы возможна при условии наличия у нарушителя прав в дискредитируемой системе: установки специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации; доступа к каналам передачи данных		
4.4	117	Угроза перехвата привилегированного потока/ КДЦ	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к потоку данных, созданного приложением с дополнительными привилегиями (к привилегированному потоку данных) путем синхронного (вызов привилегированной функции, возвращающей неправильное значение) или асинхронного (создание обратных вызовов, манипулирование указателями и т.п.) деструктивного программного воздействия на него. Данная угроза обусловлена уязвимостями программного обеспечения, использующего в своей работе участки кода, исполняемого с дополнительными правами, наследуемыми создаваемыми привилегированными потоками (наличие ошибочных указателей, некорректное освобождение памяти и т.п.). Реализация данной угрозы возможна в следующих условиях: в дискредитируемом приложении существуют участки кода, требующие исполнения с правами, превышающими права	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			обычных пользователей; нарушитель обладает привилегиями, позволяющими вносить изменения во входные данные дискредитируемого приложения		
4.5	119	Угроза перехвата управления гипервизором/ КДЦ	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счет получения нарушителем права управления гипервизором путем 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
4.6	139	Угроза преодоления физической защиты/ КДЦ	Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путем	Внешний нарушитель со средним потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			преодоления системы контроля физического доступа, организованной в здании предприятия. Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.). Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.)		
4.7	187	Угроза несанкционированного воздействия на средство защиты информации/ КДЦ	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к программной среде управления средством защиты информации и изменения режима его функционирования. Угроза обусловлена наличием у средств защиты информации программной среды управления и взаимодействия с пользователями системы. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации
4.8	193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика/	Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных. Данная у гроза обусловлена слабостями мер защиты информации при хранении, обработке и передаче информационных ресурсов. Реализация данной угрозы возможна:	Внешний нарушитель со средним потенциалом	Информационные ресурсы, объекты файловой системы

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		К	при условии успешного внедрения в дискредитируемую систему указанного вредоносного программного обеспечения; при отсутствии или недостаточной реализации мер межсетевого экранирования		
4.9	198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов/ Ц	Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	Внешний нарушитель со средним потенциалом	Система управления доступом, встроенная в операционную систему компьютера (программное обеспечение)
4.10	217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения/	Угроза заключается в возможности внедрения вредоносного кода в информационную систему за счет использования скомпрометированных доверенных источников обновлений программного обеспечения. Реализация данной угрозы возможна при использовании	Внутренний нарушитель со средним потенциалом Внешний нарушитель	Информационная система, файлы

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		КДЦ	скомпрометированных доверенных серверов обновлений программного обеспечения	со средним потенциалом	
5	Угрозы, реализуемые с использованием интернет-технологий				
5.1	42	Угроза межсайтовой подделки запроса/ КДЦ	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение
5.2	92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу TCP/IP) доступа. Данная угроза обусловлена невозможностью контроля за механизмом, реализующего функции удалённого доступа на аппаратном уровне, на уровне операционной системы, а также независимостью от состояния питания аппаратных устройств,	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			т.к. данный механизм предусматривает процедуру удалённого включения/выключения аппаратных устройств. Реализация данной угрозы возможна в условиях: наличия в системе аппаратного обеспечения, поддерживающего технологию удалённого внеполосного доступа; наличия подключения системы к сетям общего пользования (сети Интернет)		
5.3	190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет/ КДЦ	Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещаемые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты, а также отсутствием правил межсетевого экранирования. Реализация данной угрозы возможна при: неограниченном доступе пользователя в сеть Интернет; наличии у нарушителя сведений о сайтах, посещаемых пользователем	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение
5.4	197	Угроза хищения аутентификационной информации из временных файлов cookie/ К	Угроза заключается в возможности хищения с использованием вредоносной программы аутентификационной информации пользователей, их счетов, хранящейся во временных файлах cookie, и передачи этой информации нарушителям через открытый RDP-порт.	Внешний нарушитель со средним потенциалом	Информация, хранящаяся на компьютере во временных файлах (программное обеспечение)

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			Данная угроза обусловлена недостаточностью мер антивирусной защиты, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена непринятием мер по стиранию остаточной информации из временных файлов (очистке временных файлов). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт		
5.5	201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере/ К	Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнение форм авторизации. Реализация данной угрозы обусловлена хранением в браузерах в открытом виде пользовательских данных, используемых для автозаполнения форм авторизации. Реализация данной угрозы возможна при условии, что пользователь использует браузер, в котором реализована и активирована функция автоматического заполнения форм авторизации	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обеспечение)
5.6	203	Угроза утечки информации с неподключенных к сети Интернет компьютеров/	Угроза заключается в возможности хищения данных с неподключенных к сети Интернет компьютеров за счет компрометации их аппаратных элементов или устройств коммутационного оборудования (например, маршрутизаторов), оснащенных LED-индикаторами, фиксации	Внутренний нарушитель со средним потенциалом	Программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		К	мерцания этих индикаторов и расшифровки полученных результатов. Реализация данной угрозы обусловлена тем, что существует возможность несанкционированного получения управления этими индикаторами (с помощью специальной прошивки или повышения привилегий и выполнения вредоносного кода), позволяющего передавать информацию путем ее преобразования в последовательность сигналов индикаторов компьютеров и коммутационного оборудования. Реализация данной угрозы возможна при условии, что злоумышленником получен физический доступ к компрометируемому компьютеру или коммутационному оборудованию для установки средства визуального съема сигналов LED-индикаторов	Внешний нарушитель со средним потенциалом	
6	Угрозы доступа, реализуемые в виртуальной инфраструктуре				
6.1	10	Угроза выхода процесса за пределы виртуальной машины / КЦД	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	Внутренний нарушитель со средним потенциалом; внешний нарушитель со средним потенциалом	Информационная система, сетевой узел, носитель информации, объекты файловой системы, учетные данные пользователя, образ виртуальной машины

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора		
6.2	44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины/ КДЦ	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 счет эксплуатации уязвимостей гипервизора, но и путем осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы	Внутренний нарушитель со средним потенциалом; внешний нарушитель со средним потенциалом	Виртуальная машина, гипервизор
6.3	48	Угроза нарушения технологии обработки информации путем несанкционированного	Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через	Внутренний нарушитель с низким потенциалом;	Образ виртуальной машины, сетевой узел, сетевое программное

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		внесения изменений в образы виртуальных машин/ КДЦ	нее на другие системы путем 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 измененных образов; к нарушению целостности программ, установленных на виртуальных машинах; к нарушению доступности ресурсов виртуальных машин; к созданию ботнета путем внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы)	внешний нарушитель со средним потенциалом	обеспечение, виртуальная машина
6.4	73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической	Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путем 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	Внутренний нарушитель со средним потенциалом; внешний нарушитель со средним потенциалом	Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		и (или) виртуальной сети/ КДЦ	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		
6.5	76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети/ Д	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» путем 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:	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Гипервизор

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью		
6.6	77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение/ ДЦ	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 ее (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 ее 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	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Сервер, рабочая станция, виртуальная машина, гипервизор, машинный носитель информации, метаданные

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			зарезервированного под пользовательские данные адресного пространства данной виртуальной машины		
6.7	80	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети/ КДЦ	Угроза заключается в возможности удаленного 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 удаленного 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
6.8	85	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации/ К	Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределенных файлах, содержащих защищаемую информацию, путем восстановления данных распределенных файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределенной информации. Данная угроза обусловлена тем, что в связи с применением множества технологий виртуализации, предназначенных	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Носитель информации, объекты файловой системы

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			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		
6.9	120	Угроза перехвата управления средой виртуализации/ КДЦ	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым всеми гипервизорами, реализующими среду виртуализации, за счет получения нарушителем права управления этими гипервизорами путем 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	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			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		
7	Угрозы использования мобильных технических средств				
7.1	184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства/ К	Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счет использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложностью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать:	Внутренний нарушитель со средним потенциалом	Мобильное устройство

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
			персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); данные об окружающей среде (текущее местоположение мобильного устройства, маршруты движения, наличие беспроводных сетей в радиусе доступа); видеоданные, снимаемые видеокамерами мобильного устройства; аудиоданные, снимаемые микрофоном устройства		
7.2	194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Угроза заключается в возможности снятия нарушителем предустановленных производителем ограничений на конфигурирование привилегированных функций мобильного устройства. Данная угроза обусловлена наличием уязвимостей в операционных системах мобильного устройства, позволяющих получить доступ к настройкам привилегированных функций. Реализация данной угрозы возможна при получении нарушителем доступа к мобильному устройству	Внешний нарушитель с высоким потенциалом	Мобильное устройство
7.3	196	Угроза контроля вредоносной программой списка приложений,	Угроза заключается в возможности использования вредоносной программы для контроля списка приложений, запущенных на мобильном устройстве.	Внешний нарушитель с высоким потенциалом	Мобильное устройство

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
		запущенных на мобильном устройстве	Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносных программ (отсутствие контроля разрешенного программного обеспечения). Реализация данной угрозы возможна при условии, что вредоносная программа внедрена на мобильном устройстве и непреднамеренно запущена самим пользователем		
7.4	199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов/ КД	Угроза заключается в возможности управления мобильным устройством и запущенными на нем приложениями от имени легального пользователя за счет передачи этих команд через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающийся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть, не отключен) и установлена низкая чувствительность голосового идентификатора	Внешний нарушитель со средним потенциалом	Мобильное устройство и запущенные на нем приложения (программное обеспечение, аппаратное устройство)

№ п/п	Номер угрозы в банке УБИ	Наименование угрозы/нарушаемое свойство БИ конфиденциальность (К), доступность (Д), целостность (Ц)	Содержание угрозы	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия
1	2	3	4	5	6
7.5	200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов/ К	Угроза заключается в возможности хищения данных пользователя с его мобильного устройства через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающейся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (т.е. не отключен) и установлена низкая чувствительность голосового идентификатора	Внешний нарушитель со средним потенциалом	Данные пользователя мобильного устройства (аппаратное устройство)