|  |  |  |  |
| --- | --- | --- | --- |
| **Номер УБИ** | **Наименование УБИ** | **Категория нарушителя и его возможность** | **Какое свойство информации нарушает** |
| УБИ.003 | Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц |
| УБИ.004 | Угроза аппаратного сброса пароля BIOS | Внутренний нарушитель с низким потенциалом | Ц |
| УБИ.005 | Угроза внедрения вредоносного кода в BIOS | Внутренний нарушитель с высоким потенциалом | К  Ц  Д |
| УБИ.006 | Угроза внедрения кода или данных | Внешний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.007 | Угроза воздействия на программы с высокими привилегиями | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц |
| УБИ.008 | Угроза восстановления и/или повторного использования аутентификационной информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.009 | Угроза восстановления предыдущей уязвимой версии BIOS | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.011 | Угроза деавторизации санкционированного клиента беспроводной сети | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.012 | Угроза деструктивного изменения конфигурации/среды окружения программ | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.013 | Угроза деструктивного использования декларированного функционала BIOS | Внутренний нарушитель с низким потенциалом | Ц |
| УБИ.014 | Угроза длительного удержания вычислительных ресурсов пользователями | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.015 | Угроза доступа к защищаемым файлам с использованием обходного пути | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.016 | Угроза доступа к локальным файлам сервера при помощи URL | Внешний нарушитель со средним потенциалом | К |
| УБИ.017 | Угроза доступа/перехвата/изменения HTTP cookies | Внешний нарушитель с низким потенциалом | К  Д |
| УБИ.018 | Угроза загрузки нештатной операционной системы | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.019 | Угроза заражения DNS-кеша | Внешний нарушитель с низким потенциалом | К |
| УБИ.022 | Угроза избыточного выделения оперативной памяти | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.023 | Угроза изменения компонентов информационной (автоматизированной) системы | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.024 | Угроза изменения режимов работы аппаратных элементов компьютера | Внутренний нарушитель с высоким потенциалом | Ц  Д |
| УБИ.025 | Угроза изменения системных и глобальных переменных | Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.026 | Угроза искажения XML-схемы | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.027 | Угроза искажения вводимой и выводимой на периферийные устройства информации | Внешний нарушитель с высоким потенциалом  Внутренний нарушитель с низким потенциалом | Ц |
| УБИ.028 | Угроза использования альтернативных путей доступа к ресурсам | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.029 | Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.030 | Угроза использования информации идентификации/аутентификации, заданной по умолчанию | Внутренний нарушитель с низким потенциалом  Внешний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.031 | Угроза использования механизмов авторизации для повышения привилегий | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.032 | Угроза использования поддельных цифровых подписей BIOS | Внешний нарушитель со средним потенциалом | Ц |
| УБИ.033 | Угроза использования слабостей кодирования входных данных | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.034 | Угроза использования слабостей протоколов сетевого/локального обмена данными | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.035 | Угроза использования слабых криптографических алгоритмов BIOS | Внешний нарушитель с высоким потенциалом | К  Ц  Д |
| УБИ.036 | Угроза исследования механизмов работы программы | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Д |
| УБИ.037 | Угроза исследования приложения через отчёты об ошибках | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К |
| УБИ.038 | Угроза исчерпания вычислительных ресурсов хранилища больших данных | Внутренний нарушитель с низким потенциалом | Д |
| УБИ.039 | Угроза исчерпания запаса ключей, необходимых для обновления BIOS | Внешний нарушитель со средним потенциалом | Ц |
| УБИ.041 | Угроза межсайтового скриптинга | Внешний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.042 | Угроза межсайтовой подделки запроса | Внешний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.045 | Угроза нарушения изоляции среды исполнения BIOS | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.046 | Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Д |
| УБИ.048 | Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.049 | Угроза нарушения целостности данных кеша | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.050 | Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Внутренний нарушитель с низким потенциалом | Ц |
| УБИ.051 | Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания | Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.053 | Угроза невозможности управления правами пользователей BIOS | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.059 | Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.060 | Угроза неконтролируемого уничтожения информации хранилищем больших данных | Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.061 | Угроза некорректного задания структуры данных транзакции | Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.062 | Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | Внешний нарушитель с низким потенциалом | К |
| УБИ.063 | Угроза некорректного использования функционала программного и аппаратного обеспечения | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.067 | Угроза неправомерного ознакомления с защищаемой информацией | Внутренний нарушитель с низким потенциалом | К |
| УБИ.068 | Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.069 | Угроза неправомерных действий в каналах связи | Внешний нарушитель с низким потенциалом | К  Ц |
| УБИ.071 | Угроза несанкционированного восстановления удалённой защищаемой информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.072 | Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.073 | Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.074 | Угроза несанкционированного доступа к аутентификационной информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.075 | Угроза несанкционированного доступа к виртуальным каналам передачи | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.082 | Угроза несанкционированного доступа к сегментам вычислительного поля | Внутренний нарушитель со средним потенциалом | К  Ц |
| УБИ.083 | Угроза несанкционированного доступа к системе по беспроводным каналам | Внешний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.084 | Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.085 | Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К |
| УБИ.086 | Угроза несанкционированного изменения аутентификационной информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.087 | Угроза несанкционированного использования привилегированных функций BIOS | Внешний нарушитель с высоким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.088 | Угроза несанкционированного копирования защищаемой информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.089 | Угроза несанкционированного редактирования реестра | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.090 | Угроза несанкционированного создания учётной записи пользователя | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.091 | Угроза несанкционированного удаления защищаемой информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.092 | Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | Внешний нарушитель с высоким потенциалом | К  Ц  Д |
| УБИ.093 | Угроза несанкционированного управления буфером | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.094 | Угроза несанкционированного управления синхронизацией и состоянием | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.095 | Угроза несанкционированного управления указателями | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.097 | Угроза несогласованности правил доступа к большим данным | Внутренний нарушитель с низким потенциалом | К  Д |
| УБИ.098 | Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб | Внешний нарушитель с низким потенциалом | К |
| УБИ.098 | Угроза обнаружения хостов | Внешний нарушитель с низким потенциалом | К |
| УБИ.100 | Угроза обхода некорректно настроенных механизмов аутентификации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.102 | Угроза опосредованного управления группой программ через совместно используемые данные | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.103 | Угроза определения типов объектов защиты | Внешний нарушитель с низким потенциалом | К |
| УБИ.104 | Угроза определения топологии вычислительной сети | Внешний нарушитель с низким потенциалом | К |
| УБИ.105 | Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.106 | Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Внутренний нарушитель с низким потенциалом | Д |
| УБИ.107 | Угроза отключения контрольных датчиков | Внешний нарушитель с высоким потенциалом  Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.109 | Угроза перебора всех настроек и параметров приложения | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.113 | Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.115 | Угроза перехвата вводимой и выводимой на периферийные устройства информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К |
| УБИ.116 | Угроза перехвата данных, передаваемых по вычислительной сети | Внешний нарушитель с низким потенциалом | К |
| УБИ.117 | Угроза перехвата привилегированного потока | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.118 | Угроза перехвата привилегированного процесса | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.121 | Угроза повреждения системного реестра | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.122 | Угроза повышения привилегий | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.123 | Угроза подбора пароля BIOS | Внутренний нарушитель с низким потенциалом | К  Д |
| УБИ.124 | Угроза подделки записей журнала регистрации событий | Угроза подделки записей журнала регистрации событий | Ц |
| УБИ.126 | Угроза подмены беспроводного клиента или точки доступа | Внешний нарушитель с низким потенциалом | К  Д |
| УБИ.127 | Угроза подмены действия пользователя путём обмана | Внешний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.129 | Угроза подмены резервной копии программного обеспечения BIOS | Внутренний нарушитель с низким потенциалом | Ц |
| УБИ.130 | Угроза подмены содержимого сетевых ресурсов | Внешний нарушитель с низким потенциалом | К |
| УБИ.131 | Угроза подмены субъекта сетевого доступа | Внешний нарушитель со средним потенциалом | К  Ц |
| УБИ.132 | Угроза получения предварительной информации об объекте защиты | Внешний нарушитель со средним потенциалом | К |
| УБИ.136 | Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.139 | Угроза преодоления физической защиты | Внешний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.140 | Угроза приведения системы в состояние «отказ в обслуживании» | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.143 | Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.144 | Угроза программного сброса пароля BIOS | Внутренний нарушитель с низким потенциалом | К  Ц |
| УБИ.146 | Угроза прямого обращения к памяти вычислительного поля суперкомпьютера | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К |
| УБИ.150 | Угроза сбоя процесса обновления BIOS | Внутренний нарушитель со средним потенциалом | Д |
| УБИ.151 | Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | Внешний нарушитель с низким потенциалом | К |
| УБИ.152 | Угроза удаления аутентификационной информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.154 | Угроза установки уязвимых версий обновления программного обеспечения BIOS | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.155 | Угроза утраты вычислительных ресурсов | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Д |
| УБИ.157 | Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | Внешний нарушитель с низким потенциалом | Ц  Д |
| УБИ.159 | Угроза «форсированного веб-браузинга» | Внешний нарушитель с низким потенциалом | К |
| УБИ.161 | Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями | Внутренний нарушитель с низким потенциалом | Д |
| УБИ.165 | Угроза включения в проект не достоверно испытанных компонентов | Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.166 | Угроза внедрения системной избыточности | Внутренний нарушитель со средним потенциалом | Д |
| УБИ.167 | Угроза заражения компьютера при посещении неблагонадёжных сайтов | Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.168 | Угроза «кражи» учётной записи доступа к сетевым сервисам | Внешний нарушитель с низким потенциалом | К  Д |
| УБИ.169 | Угроза наличия механизмов разработчика | Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.170 | Угроза неправомерного шифрования информации | Внешний нарушитель с низким потенциалом | Д |
| УБИ.172 | Угроза распространения «почтовых червей» | Внешний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.173 | Угроза «спама» веб-сервера | Внешний нарушитель с низким потенциалом | Д |
| УБИ.174 | Угроза «фарминга» | Внешний нарушитель с низким потенциалом | К |
| УБИ.175 | Угроза «фишинга» | Внешний нарушитель с низким потенциалом | К |
| УБИ.176 | Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты | Внешний нарушитель с низким потенциалом | Д |
| УБИ.177 | Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью | Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.178 | Угроза несанкционированного использования системных и сетевых утилит | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц  Д |
| УБИ.179 | Угроза несанкционированной модификации защищаемой информации | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | Ц |
| УБИ.180 | Угроза отказа подсистемы обеспечения температурного режима | Внутренний нарушитель с низким потенциалом  Внешний нарушитель со средним потенциалом | Д |
| УБИ.181 | Угроза перехвата одноразовых паролей в режиме реального времени | Внешний нарушитель со средним потенциалом | Ц |
| УБИ.182 | Угроза физического устаревания аппаратных компонентов | Внутренний нарушитель с низким потенциалом | Д |
| УБИ.183 | Угроза перехвата управления автоматизированной системой управления технологическими процессами | Внешний нарушитель с высоким потенциалом  Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.186 | Угроза внедрения вредоносного кода через рекламу, сервисы и контент | Внутренний нарушитель с низким потенциалом | Ц  Д |
| УБИ.187 | Угроза несанкционированного воздействия на средство защиты информации | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.190 | Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет | Внешний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.197 | Угроза хищения аутентификационной информации из временных файлов cookie | Внешний нарушитель со средним потенциалом | К |
| УБИ.201 | Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере | Внешний нарушитель со средним потенциалом | К |
| УБИ.209 | Угроза несанкционированного доступа к защищаемой памяти ядра процессора | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | К  Ц Д |
| УБИ.210 | Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения | Внутренний нарушитель с высоким потенциалом | Ц  Д |
| УБИ.211 | Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем | Внутренний нарушитель с низким потенциалом | К  Ц |
| УБИ.212 | Угроза перехвата управления информационной системой | Внутренний нарушитель со средним потенциалом | К  Ц  Д |
| УБИ.213 | Угроза обхода многофакторной аутентификации | Внешний нарушитель с высоким потенциалом | К  Ц  Д |
| УБИ.214 | Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации | Внутренний нарушитель со средним потенциалом | Ц  Д |
| УБИ.215 | Угроза несанкционированного доступа к системе при помощи сторонних сервисов | Внешний нарушитель со средним потенциалом | К  Ц  Д |