**ДЕПАРТАМЕНТ ИМУЩЕСТВЕННЫХ ОТНОШЕНИЙ ВОЛОГОДСКОЙ ОБЛАСТИ**

# П Р И К А З

28.05.2020 № 48 -н

Об утверждении перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Департаменте имущественных отношений Вологодской области

С целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Департаменте имущественных отношений Вологодской области, в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Департамента имущественных отношений Вологодской области (приложение).

2. Настоящий приказ вступает в силу после его подписания.

Начальник Департамента Л.В. Балаева

Приложение
к приказу Департамента
имущественных отношений
Вологодской области
от 28.05.2020 № 48 -н

**ПЕРЕЧЕНЬ**

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Департамента имущественных отношений Вологодской области

| № п/п | Идентификатор УБИ | Наименование угрозы информационной безопасности |
|---|---|---|
| 1 | УБИ 004 | Угроза аппаратного сброса пароля BIOS |
| 2 | УБИ 006 | Угроза внедрения кода или данных |
| 3 | УБИ 008 | Угроза восстановления аутентификационной информации |
| 4 | УБИ 009 | Угроза восстановления предыдущей уязвимой версии BIOS |
| 5 | УБИ 012 | Угроза деструктивного изменения конфигурации/среды окружения программ |
| 6 | УБИ 013 | Угроза деструктивного использования декларированного функционала BIOS |
| 7 | УБИ 014 | Угроза длительного удержания вычислительных ресурсов пользователями |
| 8 | УБИ 015 | Угроза доступа к защищаемым файлам с использованием обходного пути |
| 9 | УБИ 017 | Угроза доступа/перехвата/изменения HTTP cookies |
| 10 | УБИ 018 | Угроза загрузки нештатной операционной системы |
| 11 | УБИ 019 | Угроза заражения DNS-кеша |
| 12 | УБИ 022 | Угроза избыточного выделения оперативной памяти |
| 13 | УБИ 023 | Угроза изменения компонентов системы |
| 14 | УБИ 027 | Угроза искажения вводимой и выводимой на периферийные устройства информации |
| 15 | УБИ 028 | Угроза использования альтернативных путей доступа к ресурсам |
| 16 | УБИ 030 | Угроза использования информации идентификации/аутентификации, заданной по умолчанию |
| 17 | УБИ 031 | Угроза использования механизмов авторизации для повышения привилегий |
| 18 | УБИ 034 | Угроза использования слабостей протоколов сетевого/локального обмена данными |
| 19 | УБИ 041 | Угроза межсайтового скриптинга |
| 20 | УБИ 045 | Угроза нарушения изоляции среды исполнения BIOS |

| | | |
|---|---|---|
| 21 | УБИ 046 | Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия |
| 22 | УБИ 049 | Угроза нарушения целостности данных кеша |
| 23 | УБИ 051 | Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания |
| 24 | УБИ 053 | Угроза невозможности управления правами пользователей BIOS |
| 25 | УБИ 059 | Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов |
| 26 | УБИ 062 | Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера |
| 27 | УБИ 067 | Угроза неправомерного ознакомления с защищаемой информацией |
| 28 | УБИ 069 | Угроза неправомерных действий в каналах связи |
| 29 | УБИ 071 | Угроза несанкционированного восстановления удалённой защищаемой информации |
| 30 | УБИ 072 | Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS |
| 31 | УБИ 074 | Угроза несанкционированного доступа к аутентификационной информации |
| 32 | УБИ 075 | Угроза несанкционированного доступа к виртуальным каналам передачи |
| 33 | УБИ 078 | Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети |
| 34 | УБИ 079 | Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин |
| 35 | УБИ 084 | Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети |
| 36 | УБИ 086 | Угроза несанкционированного изменения аутентификационной информации |
| 37 | УБИ 087 | Угроза несанкционированного использования привилегированных функций BIOS |
| 38 | УБИ 088 | Угроза несанкционированного копирования защищаемой информации |
| 39 | УБИ 089 | Угроза несанкционированного редактирования реестра |
| 40 | УБИ 090 | Угроза несанкционированного создания учётной записи пользователя |
| 41 | УБИ 091 | Угроза несанкционированного удаления защищаемой информации |
| 42 | УБИ 093 | Угроза несанкционированного управления буфером |
| 43 | УБИ 098 | Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб |

| | | |
|---|---|---|
| 44 | УБИ 099 | Угроза обнаружения хостов |
| 45 | УБИ 100 | Угроза обхода некорректно настроенных механизмов аутентификации |
| 46 | УБИ 103 | Угроза определения типов объектов защиты |
| 47 | УБИ 104 | Угроза определения топологии вычислительной сети |
| 48 | УБИ 108 | Угроза ошибки обновления гипервизора |
| 49 | УБИ 113 | Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники |
| 50 | УБИ 115 | Угроза перехвата вводимой и выводимой на периферийные устройства информации |
| 51 | УБИ 116 | Угроза перехвата данных, передаваемых по вычислительной сети |
| 52 | УБИ 121 | Угроза повреждения системного реестра |
| 53 | УБИ 123 | Угроза подбора пароля BIOS |
| 54 | УБИ 124 | Угроза подделки записей журнала регистрации событий |
| 55 | УБИ 128 | Угроза подмены доверенного пользователя |
| 56 | УБИ 129 | Угроза подмены резервной копии программного обеспечения BIOS |
| 57 | УБИ 130 | Угроза подмены содержимого сетевых ресурсов |
| 58 | УБИ 140 | Угроза приведения системы в состояние «отказ в обслуживании» |
| 59 | УБИ 144 | Угроза программного сброса пароля BIOS |
| 60 | УБИ 145 | Угроза пропуска проверки целостности программного обеспечения |
| 61 | УБИ 151 | Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL |
| 62 | УБИ 152 | Угроза удаления аутентификационной информации |
| 63 | УБИ 153 | Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов |
| 64 | УБИ 155 | Угроза утраты вычислительных ресурсов |
| 65 | УБИ 156 | Угроза утраты носителей информации |
| 66 | УБИ 157 | Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации |
| 67 | УБИ 158 | Угроза форматирования носителей информации |
| 68 | УБИ 159 | Угроза «форсированного веб-браузинга» |
| 69 | УБИ 160 | Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации |
| 70 | УБИ 162 | Угроза эксплуатации цифровой подписи программного кода |
| 71 | УБИ 167 | Угроза заражения компьютера при посещении неблагонадёжных сайтов |
| 72 | УБИ 168 | Угроза «кражи» учётной записи доступа к сетевым сервисам |
| 73 | УБИ 170 | Угроза неправомерного шифрования информации |
| 74 | УБИ 171 | Угроза скрытного включения вычислительного устройства в состав бот-сети |

| | | |
|---|---|---|
| 75 | УБИ 172 | Угроза распространения «почтовых червей» |
| 76 | УБИ 173 | Угроза «спама» веб-сервера |
| 77 | УБИ 174 | Угроза «фарминга» |
| 78 | УБИ 175 | Угроза «фишинга» |
| 79 | УБИ 177 | Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью |
| 80 | УБИ 178 | Угроза несанкционированного использования системных и сетевых утилит |
| 81 | УБИ 179 | Угроза несанкционированной модификации защищаемой информации |
| 82 | УБИ 180 | Угроза отказа подсистемы обеспечения температурного режима |
| 83 | УБИ 182 | Угроза физического устаревания аппаратных компонентов |
| 84 | УБИ 185 | Угроза несанкционированного изменения параметров настройки средств защиты информации |
| 85 | УБИ 186 | Угроза внедрения вредоносного кода через рекламу, сервисы и контент |
| 86 | УБИ 191 | Угроза внедрения вредоносного кода в дистрибутив программного обеспечения |
| 87 | УБИ 192 | Угроза использования уязвимых версий программного обеспечения |
| 88 | УБИ 205 | Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты |
| 89 | УБИ 208 | Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники |
| 90 | УБИ 209 | Угроза несанкционированного доступа к защищаемой памяти ядра процессора |
| 91 | УБИ 211 | Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем |