**ПРАВИТЕЛЬСТВО АЛТАЙСКОГО КРАЯ**

# ПОСТАНОВЛЕНИЕ

28.06.2022 № 234

г. Барнаул

О внесении изменений в постановление Правительства Алтайского края от 24.09.2019 № 356

Правительство Алтайского края п о с т а н о в л я е т:

Внести в постановление Правительства Алтайского края от 24.09.2019 № 356 «Об определении угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных органов исполнительной власти Алтайского края» следующие изменения:

пункт 2 изложить в следующей редакции:

«2. Органам исполнительной власти Алтайского края, а также подведомственным им учреждениям при определении угроз безопасности персональных данных при их обработке в информационных системах руководствоваться Перечнем с учетом структурно-функциональных характеристик информационных систем.»;

перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Алтайского края при осуществлении ими соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки, утвержденный указанным постановлением, изложить в редакции согласно приложению к настоящему постановлению.

Губернатор Алтайского края,
Председатель Правительства
Алтайского края В.П. Томенко

ПРАВИТЕЛЬСТВО АЛТАЙСКОГО КРАЯ
ДЛЯ ДОКУМЕНТОВ
2

ПРИЛОЖЕНИЕ
к постановлению Правительства
Алтайского края
от 28.06. 2022 №234

# ПЕРЕЧЕНЬ
## угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в органах исполнительной власти Алтайского края при осуществлении ими соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

| № п/п | Наименование угрозы |
|---|---|
| 1 | 2 |
| 1 | Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям ФСТЭК России |
| 1.1 | отсутствие аутентификации пользователей компьютеров до загрузки операционной системы (паролей BIOS, дополнительных аппаратных средств аутентификации) |
| 1.2 | разглашение паролей BIOS или дополнительных аппаратных средств аутентификации, например, записывание в доступном для нарушителя месте (на бумаге, клавиатуре и т.п.) |
| 1.3 | использование технологического пароля BIOS |
| 1.4 | предоставление пользователям прав доступа (в том числе по видам доступа) к персональным данным и другим ресурсам информационных систем персональных данных сверх необходимого для работы |
| 1.5 | отправка персональных данных по ошибочным адресам электронной почты |
| 1.6 | разглашение (например, при разговорах, записывание на бумаге и т.п.) пользовательских имён и паролей |
| 1.7 | использование для входа в систему чужих идентификаторов и паролей |
| 1.8 | формирование недекларированных возможностей программного обеспечения |
| 1.9 | внедрение вредоносных программ, распространяющихся по сети (сетевые черви), которые реализуют передачу своего кода на удаленный сервер или рабочую станцию |
| 1.10 | передача по сетям за пределами контролируемой территории персональных данных и иной конфиденциальной информации в открытом (или слабо защищённом) виде |
| 1.11 | сбор информации об объектах сети |
| 1.12 | активизация распространяемых злоумышленниками файлов при случайном обращении к ним пользователя |
| 1.13 | переполнение буфера приложений-серверов; использование недостатков программ, реализующих сетевые сервисы: настройка системных регистров, позволяющая переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера |
| 1.14 | использование возможностей удаленного управления системой. Использование скрытых компонентов («троянских» программ) либо штатных средств управления и администрирования компьютерных сетей |

| 1 | 2 |
|---|---|
| 1.15 | подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа (IP-spoofing) |
| 1.16 | нарушение логической связности между атрибутами, данными, объектами; передача нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации |
| 1.17 | использование ошибок в программах; передача пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер |
| 1.18 | атаки на DNS |
| 1.19 | атаки на ARP |
| 1.20 | ошибки при разработке или доработке программного обеспечения информационных систем персональных данных (в том числе средств защиты информации) |
| 1.21 | преднамеренное внесение в программы при их разработке или доработке вредоносных кодов (программные закладки) |
| 1.22 | осуществление неавторизованных действий в серверном помещении |
| 1.23 | осуществление неавторизованных действий в помещениях, в которых осуществляется обработка персональных данных |
| 1.24 | ошибки при обслуживании серверного оборудования и проведении операций по обслуживанию прикладных систем либо при проведении установочных работ |
| 1.25 | хищение, утрата резервных копий носителей баз данных персональных данных |
| 1.26 | нарушение порядка резервного копирования персональных данных |
| 1.27 | доступ к информации информационных систем персональных данных, выходящей за пределы контролируемой зоны вследствие списания (утилизации) носителей информации, содержащих персональные данные |
| 1.28 | уничтожение данных в информационных системах персональных данных или блокирование доступа к информационным системам персональных данных, вызванное стихийными бедствиями или техногенными катастрофами |
| 1.29 | сбой системы электроснабжения информационных систем персональных данных |
| 1.30 | нарушение изоляции пользовательских данных внутри виртуальной машины |
| 1.31 | нарушение технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин |
| 1.32 | угрозы безопасности информации (далее – УБИ) из состава банка данных угроз безопасности информации (bdu.fstec.ru) |
| 1.32.1 | УБИ.004: угроза аппаратного сброса пароля BIOS |
| 1.32.2 | УБИ.005: угроза внедрения вредоносного кода в BIOS |
| 1.32.3 | УБИ.006: угроза внедрения кода или данных |
| 1.32.4 | УБИ.008: угроза восстановления и/или повторного использования аутентификационной информации |
| 1.32.5 | УБИ.009: угроза восстановления предыдущей уязвимой версии BIOS |
| 1.32.6 | УБИ.011: угроза деавторизации санкционированного клиента беспроводной сети |
| 1.32.7 | УБИ.012: угроза деструктивного изменения конфигурации/среды окружения программ |
| 1.32.8 | УБИ.013: угроза деструктивного использования декларированного функционала BIOS |

| 1 | 2 |
|---|---|
| 1.32.9 | УБИ.014: угроза длительного удержания вычислительных ресурсов пользователями |
| 1.32.10 | УБИ.015: угроза доступа к защищаемым файлам с использованием обходного пути |
| 1.32.11 | УБИ.017: угроза доступа/перехвата/изменения HTTP cookies |
| 1.32.12 | УБИ.018: угроза загрузки нештатной операционной системы |
| 1.32.13 | УБИ.019: угроза заражения DNS-кеша |
| 1.32.14 | УБИ.020: угроза злоупотребления возможностями, предоставленными потребителям облачных услуг |
| 1.32.15 | УБИ.021: угроза злоупотребления доверием потребителей облачных услуг |
| 1.32.16 | УБИ.022: угроза избыточного выделения оперативной памяти |
| 1.32.17 | УБИ.023: угроза изменения компонентов информационной (автоматизированной) системы |
| 1.32.18 | УБИ.024: угроза изменения режимов работы аппаратных элементов компьютера |
| 1.32.19 | УБИ.025: угроза изменения системных и глобальных переменных |
| 1.32.20 | УБИ.028: угроза использования альтернативных путей доступа к ресурсам |
| 1.32.21 | УБИ.031: угроза использования механизмов авторизации для повышения привилегий |
| 1.32.22 | УБИ.034: угроза использования слабостей протоколов сетевого/локального обмена данными |
| 1.32.23 | УБИ.041: угроза межсайтового скриптинга |
| 1.32.24 | УБИ.043: угроза нарушения доступности облачного сервера |
| 1.32.25 | УБИ.045: угроза нарушения изоляции среды исполнения BIOS |
| 1.32.26 | УБИ.046: угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия |
| 1.32.27 | УБИ.049: угроза нарушения целостности данных кеша |
| 1.32.28 | УБИ.051: угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания |
| 1.32.29 | УБИ.052: угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения |
| 1.32.30 | УБИ.053: угроза невозможности управления правами пользователей BIOS |
| 1.32.31 | УБИ.054: угроза недобросовестного исполнения обязательств поставщиками облачных услуг |
| 1.32.32 | УБИ.055: угроза незащищённого администрирования облачных услуг |
| 1.32.33 | УБИ.056: угроза некачественного переноса инфраструктуры в облако |
| 1.32.34 | УБИ.058: угроза неконтролируемого роста числа виртуальных машин |
| 1.32.35 | УБИ.059: угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов |
| 1.32.36 | УБИ.061: угроза некорректного задания структуры данных транзакции |
| 1.32.37 | УБИ.062: угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера |
| 1.32.38 | УБИ.064: угроза некорректной реализации политики лицензирования в облаке |
| 1.32.39 | УБИ.065: угроза неопределённости в распределении ответственности между ролями в облаке |
| 1.32.40 | УБИ.066: угроза неопределённости ответственности за обеспечение безопасности облака |
| 1.32.41 | УБИ.067: угроза неправомерного ознакомления с защищаемой информацией |
| 1.32.42 | УБИ.069: угроза неправомерных действий в каналах связи |
| 1.32.43 | УБИ.070: угроза непрерывной модернизации облачной инфраструктуры |

| 1 | 2 |
|---|---|
| 1.32.44 | УБИ.071: угроза несанкционированного восстановления удалённой защищаемой информации |
| 1.32.45 | УБИ.072: угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS |
| 1.32.46 | УБИ.074: угроза несанкционированного доступа к аутентификационной информации |
| 1.32.47 | УБИ.075: угроза несанкционированного доступа к виртуальным каналам передачи |
| 1.32.48 | УБИ.078: угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети |
| 1.32.49 | УБИ.079: угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин |
| 1.32.50 | УБИ.083: угроза несанкционированного доступа к системе по беспроводным каналам |
| 1.32.51 | УБИ.084: угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети |
| 1.32.52 | УБИ.086: угроза несанкционированного изменения аутентификационной информации |
| 1.32.53 | УБИ.088: угроза несанкционированного копирования защищаемой информации |
| 1.32.54 | УБИ.089: угроза несанкционированного редактирования реестра |
| 1.32.55 | УБИ.090: угроза несанкционированного создания учётной записи пользователя |
| 1.32.56 | УБИ.091: угроза несанкционированного удаления защищаемой информации |
| 1.32.57 | УБИ.093: угроза несанкционированного управления буфером |
| 1.32.58 | УБИ.096: угроза несогласованности политик безопасности элементов облачной инфраструктуры |
| 1.32.59 | УБИ.098: угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб |
| 1.32.60 | УБИ.099: угроза обнаружения хостов |
| 1.32.61 | УБИ.100: угроза обхода некорректно настроенных механизмов аутентификации |
| 1.32.62 | УБИ.103: угроза определения типов объектов защиты |
| 1.32.63 | УБИ.104: угроза определения топологии вычислительной сети |
| 1.32.64 | УБИ.108: угроза ошибки обновления гипервизора |
| 1.32.65 | УБИ.112: угроза передачи запрещённых команд на оборудование с числовым программным управлением |
| 1.32.66 | УБИ.113: угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники |
| 1.32.67 | УБИ.115: угроза перехвата вводимой и выводимой на периферийные устройства информации |
| 1.32.68 | УБИ.116: угроза перехвата данных, передаваемых по вычислительной сети |
| 1.32.69 | УБИ.121: угроза повреждения системного реестра |
| 1.32.70 | УБИ.123: угроза подбора пароля BIOS |
| 1.32.71 | УБИ.124: угроза подделки записей журнала регистрации событий |
| 1.32.72 | УБИ.125: угроза подключения к беспроводной сети в обход процедуры аутентификации |
| 1.32.73 | УБИ.126: угроза подмены беспроводного клиента или точки доступа |
| 1.32.74 | УБИ.128: угроза подмены доверенного пользователя |
| 1.32.75 | УБИ.129: угроза подмены резервной копии программного обеспечения BIOS |

| 1 | 2 |
|---|---|
| 1.32.76 | УБИ.130: угроза подмены содержимого сетевых ресурсов |
| 1.32.77 | УБИ.133: угроза получения сведений о владельце беспроводного устройства |
| 1.32.78 | УБИ.134: угроза потери доверия к поставщику облачных услуг |
| 1.32.79 | УБИ.135: угроза потери и утечки данных, обрабатываемых в облаке |
| 1.32.80 | УБИ.138: угроза потери управления собственной инфраструктурой при переносе её в облако |
| 1.32.81 | УБИ.140: угроза приведения системы в состояние «отказ в обслуживании» |
| 1.32.82 | УБИ.141: угроза привязки к поставщику облачных услуг |
| 1.32.83 | УБИ.142: угроза приостановки оказания облачных услуг вследствие технических сбоев |
| 1.32.84 | УБИ.144: угроза программного сброса пароля BIOS |
| 1.32.85 | УБИ.145: угроза пропуска проверки целостности программного обеспечения |
| 1.32.86 | УБИ.150: угроза сбоя процесса обновления BIOS |
| 1.32.87 | УБИ.151: угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL |
| 1.32.88 | УБИ.152: угроза удаления аутентификационной информации |
| 1.32.89 | УБИ.153: угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов |
| 1.32.90 | УБИ.155: угроза утраты вычислительных ресурсов |
| 1.32.91 | УБИ.156: угроза утраты носителей информации |
| 1.32.92 | УБИ.157: угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации |
| 1.32.93 | УБИ.158: угроза форматирования носителей информации |
| 1.32.94 | УБИ.159: угроза «форсированного веб-браузинга» |
| 1.32.95 | УБИ.160: угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации |
| 1.32.96 | УБИ.162: угроза эксплуатации цифровой подписи программного кода |
| 1.32.97 | УБИ.164: угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре |
| 1.32.98 | УБИ.165: угроза включения в проект не достоверно испытанных компонентов |
| 1.32.99 | УБИ.166: угроза внедрения системной избыточности |
| 1.32.100 | УБИ.167: угроза заражения компьютера при посещении неблагонадёжных сайтов |
| 1.32.101 | УБИ.168: угроза «кражи» учётной записи доступа к сетевым сервисам |
| 1.32.102 | УБИ.169: угроза наличия механизмов разработчика |
| 1.32.103 | УБИ.170: угроза неправомерного шифрования информации |
| 1.32.104 | УБИ.171: угроза скрытного включения вычислительного устройства в состав бот-сети |
| 1.32.105 | УБИ.172: угроза распространения «почтовых червей» |
| 1.32.106 | УБИ.173: угроза «спама» веб-сервера |
| 1.32.107 | УБИ.174: угроза «фарминга» |
| 1.32.108 | УБИ.175: угроза «фишинга» |
| 1.32.109 | УБИ.176: угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты |
| 1.32.110 | УБИ.177: угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью |
| 1.32.111 | УБИ.178: угроза несанкционированного использования системных и сетевых утилит |
| 1.32.112 | УБИ.179: угроза несанкционированной модификации защищаемой информации |

| 1 | 2 |
|---|---|
| 1.32.113 | УБИ.182: угроза физического устаревания аппаратных компонентов |
| 1.32.114 | УБИ.184: угроза агрегирования данных, обрабатываемых с помощью мобильного устройства |
| 1.32.115 | УБИ.185: угроза несанкционированного изменения параметров настройки средств защиты информации |
| 1.32.116 | УБИ.186: угроза внедрения вредоносного кода через рекламу, сервисы и контент |
| 1.32.117 | УБИ.188: угроза подмены программного обеспечения |
| 1.32.118 | УБИ.191: угроза внедрения вредоносного кода в дистрибутив программного обеспечения |
| 1.32.119 | УБИ.192: угроза использования уязвимых версий программного обеспечения |
| 1.32.120 | УБИ.205: угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты |
| 1.32.121 | УБИ.207: угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей) |
| 1.32.122 | УБИ.209: угроза несанкционированного доступа к защищаемой памяти ядра процессора |
| 1.32.123 | УБИ.210: угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения |
| 1.32.124 | УБИ.211: угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем |
| 1.32.125 | УБИ.212: угроза перехвата управления информационной системой |
| 1.32.126 | УБИ.214: угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации |
| 2 | Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям ФСБ России |
| 2.1 | реализация целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых средств криптографической защиты информации (далее – СКЗИ) персональных данных или создания условий для этого (далее – «атака») при нахождении в пределах контролируемой зоны |
| 2.2 | проведение атак на этапе эксплуатации СКЗИ на следующие объекты:<br>документацию на СКЗИ и компоненты среды функционирования СКЗИ;<br>помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и среды функционирования СКЗИ (далее – СФ) |
| 2.3 | получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:<br>сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;<br>сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;<br>сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ СКЗИ |
| 2.4 | использование штатных средств информационных систем персональных данных, ограниченное мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и |

| 1 | 2 |
|---|---|
| | пресечение несанкционированных действий |
| 2.5 | физический доступ к СВТ, на которых реализованы СКЗИ и СФ СКЗИ |
| 2.6 | возможность воздействовать на аппаратные компоненты СКЗИ и СФ СКЗИ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |
| 2.7 | создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ СКЗИ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения |
| 2.8 | проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |
| 2.9 | проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ СКЗИ, в том числе с использованием исходных текстов входящего в СФ СКЗИ прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ |
| 2.10 | создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения |
| 2.11 | возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ СКЗИ |
| 2.12 | возможность воздействовать на любые компоненты СКЗИ и СФ СКЗИ |