ПРАВИТЕЛЬСТВО АЛТАЙСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

24.09.2019 № 356

г. Барнаул

Об определении угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных органов исполнительной власти Алтайского края

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Алтайского края, Правительство Алтайского края п о с т а н о в л я е т:

1. Утвердить прилагаемый 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 (далее – «Перечень»).

2. Руководителям органов исполнительной власти Алтайского края, а также подведомственных им учреждений разрабатывать с учетом Перечня частные модели угроз безопасности персональных данных при их обработке в информационных системах.

3. Признать утратившим силу постановление Администрации Алтайского края от 20.12.2013 № 680 «О некоторых вопросах обеспечения безопасности персональных данных в системе органов исполнительной власти Алтайского края».

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

ПРАВИТЕЛЬСТВО АЛТАЙСКОГО КРАЯ
ДЛЯ ДОКУМЕНТОВ
2

ПРИЛОЖЕНИЕ

УТВЕРЖДЕН
постановлением Правительства
Алтайского края
от 24.09. 2019 № 356

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	утечка по акустическому каналу
1.2	утечка по виброакустическому каналу
1.3	утечка по виброакустическому (лазерному) каналу
1.4	утечка по акустоэлектрическому каналу
1.5	просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных (далее – ПДн)
1.6	просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных
1.7	просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн
1.8	использование специальных электронных устройств, внедренных в помещении, в котором ведется обработка ПДн
1.9	просмотр информации посредством коллективного отображения
1.10	просмотр информации с печатных документов сотрудниками, не допущенными к обработке ПДн
1.11	просмотр информации с печатных документов посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн
1.12	перехват техническими средствами побочных электромагнитных излучений информативных сигналов от технических средств и линий передачи информации
1.13	перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящих за пределы служебных помещений
1.14	перехват техническими средствами радиоизлучений, модулированных информативным сигналом, возникающих в результате работы различных генераторов в составе информационных систем персональных данных (далее – ИСПДн) или в результате паразитной генерации в узлах (элементах) технических средств
1.15	перехват техническими средствами радиоизлучений, формируемых за счет высокочастотного облучения технических средств ИСПДн
1.16	перехват техническими средствами оптического излучения с боковой поверхно-

1	2
	сти оптического волокна в волоконно-оптической системе передачи данных
1.17	применение электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн («аппаратурные закладки»)
1.18	отсутствие аутентификации пользователей компьютеров до загрузки операционной системы (далее – ОС) (паролей BIOS, дополнительных аппаратных средств аутентификации)
1.19	разглашение паролей BIOS или дополнительных аппаратных средств аутентификации, например, записывание в доступном для нарушителя месте (на бумаге, клавиатуре и т.п.)
1.20	подбор пароля BIOS (или дополнительных аппаратных средств аутентификации)
1.21	использование технологического пароля BIOS
1.22	вскрытие компьютера и аппаратный сброс пароля BIOS
1.23	некорректная реализация политики лицензирования в облаке
1.24	загрузка сторонней операционной системы (без средств защиты и разграничения доступа к ресурсам компьютера)
1.25	предоставление пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам ИСПДн сверх необходимого для работы
1.26	копирование доступных ПДн на неучтённые (в том числе отчуждаемые) носители, в том числе печать неучтённых копий документов с ПДн на принтерах
1.27	отправка ПДн по ошибочным адресам электронной почты
1.28	преднамеренное или случайное искажение (фальсификация) ПДн
1.29	несанкционированное редактирование реестра
1.30	преднамеренное или случайное уничтожение ПДн (записей, файлов, форматирование диска)
1.31	разглашение (например, при разговорах, записывание на бумаге и т.п.) пользовательских имён и паролей
1.32	внедрение аппаратного «клавиатурного шпиона»
1.33	использование для входа в систему чужих идентификаторов и паролей
1.34	оставление без присмотра незаблокированных рабочих станций
1.35	внедрение и использование неучтенных программ
1.36	преднамеренное или случайное изменение настроек и режимов работы программного обеспечения (далее – ПО), модификация ПО (удаление, искажение или подмена программных компонентов ИСПДн или систем защиты информации)
1.37	преднамеренное или случайное искажение или удаление программных компонентов системы или средств защиты информации (далее – СЗИ)
1.38	подключение к ИСПДн стороннего оборудования (компьютеров, дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи)
1.39	нарушение работоспособности технических средств обработки и защиты информации
1.40	вмешательство в работу (нарушение правил использования) средств защиты
1.41	несанкционированное изменение конфигурационных файлов ПО (настроек экрана, сети, прикладных программ)
1.42	использование сторонних носителей данных и оборудования (компьютеров, смартфонов, телефонов, фотоаппаратов, видеокамер, и иных устройств)
1.43	запуск сторонних программ
1.44	формирование недекларированных возможностей ПО
1.45	программные закладки

1	2
1.46	преднамеренная установка вредоносных программ (далее – ВП)
1.47	отключение средств антивирусной защиты пользователями
1.48	внедрение классических программных (компьютерных) вирусов, реализующих запись кода вредоносного ПО в код других программ с целью получения управления при запуске зараженных файлов, создание файлов-двойников для легального ПО, копирование кода вредоносной программы в каталоги для последующего запуска пользователем
1.49	внедрение ВП, распространяющихся по сети (сетевые черви), которые реализуют передачу своего кода на удаленный сервер или рабочую станцию
1.50	использование подключений к различным сетям (Web, почта, локальная сеть и т.п.)
1.51	передача по сетям за пределами контролируемой территории ПДн и иной конфиденциальной информации в открытом (или слабо защищённом) виде
1.52	использование программ-анализаторов пакетов (снифферов) для перехвата ПДн (и иной конфиденциальной информации)
1.53	использование программ-анализаторов пакетов (снифферов) для перехвата идентификаторов и паролей удалённого доступа (к сетевым службам)
1.54	сбор информации об объектах сети
1.55	активизация распространяемых злоумышленниками файлов при случайном обращении к ним пользователя
1.56	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
1.57	использование возможностей удаленного управления системой. Использование скрытых компонентов («троянских» программ) либо штатных средств управления и администрирования компьютерных сетей
1.58	инвентаризация сетевых ресурсов (поиск узлов сети, определение их адресов, типов ОС)
1.59	выявление сетевых служб, используемых портов, версий программ (уязвимых)
1.60	подбор идентификаторов и паролей пользователей сетевых служб (и их последующее использование)
1.61	применение методов социальной инженерии (мошенничество, обман)
1.62	подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа (IP-spoofing)
1.63	частичное исчерпание ресурсов; привлечение части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником, со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов
1.64	полное исчерпание ресурсов; исчерпание ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание)
1.65	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
1.66	использование ошибок в программах; передача пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер
1.67	атаки на DNS

1	2
1.68	атаки на ARP
1.69	внедрение ложного ARP сервера
1.70	внедрение ложного DNS сервера
1.71	фишинг
1.72	ошибки при разработке программного обеспечения ИСПДн (в том числе СЗИ)
1.73	преднамеренное внесение в программы при их разработке вредоносных кодов (программные закладки)
1.74	осуществление неавторизованных действий в серверном помещении
1.75	осуществление неавторизованных действий в помещениях, в которых осуществляется обработка ПДн
1.76	ошибки при обслуживании серверного оборудования и проведении операций по обслуживанию прикладных систем либо при проведении установочных работ
1.77	ошибки при доработке программного обеспечения ИСПДн (в том числе СЗИ)
1.78	преднамеренное внесение в программы при их доработке вредоносных кодов (программные закладки)
1.79	физическое копирование носителей баз данных (далее – БДн) ПДн
1.80	хищение, утрата резервных копий носителей БДн ПДн
1.81	нарушение порядка резервного копирования ПДн
1.82	утеря или кража оборудования ИСПДн (в том числе носителей информации)
1.83	доступ к информации ИСПДн, выходящей за пределы контролируемой зоны вследствие списания (утилизации) носителей информации, содержащих ПДн
1.84	уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами
1.85	сбой системы электроснабжения ИСПДн
1.86	угрозы безопасности информации, размещенные на официальном сайте Федеральной службы по техническому и экспортному контролю (http://bdu.fstec.ru)
1.87	использование нетрадиционных каналов (например, стеганография) для передачи ПДн
1.88	нарушение изоляции пользовательских данных внутри виртуальной машины
1.89	нарушение процедуры аутентификации субъектов виртуального информационного взаимодействия
1.90	нарушение технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин
1.91	несанкционированный доступ к виртуальным каналам передачи
1.92	несанкционированный доступ к защищаемым виртуальным машинам из виртуальной и (или) физической сети
1.93	несанкционированный доступ к защищаемым виртуальным машинам со стороны других виртуальных машин
1.94	несанкционированный доступ к системе хранения данных из виртуальной и (или) физической сети
1.95	перехват управления средой виртуализации
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

1	2
2.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования СКЗИ; 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: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ СКЗИ
2.4	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и 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