МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ
РОСТОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от «06» июля 2018 г. № 4

г. Ростов-на-Дону

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых министерством информационных технологий и связи Ростовской области и аппаратом Правительства Ростовской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Положением о министерстве информационных технологий и связи Ростовской области, утвержденным постановлением Правительства Ростовской области от 09.12.2011 № 213 министерство информационных технологий и связи Ростовской области **постановляет:**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых министерством информационных технологий и связи Ростовской области и аппаратом Правительства Ростовской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки согласно приложению.

2. Постановление вступает в силу со дня его официального опубликования.

3. Контроль за выполнением настоящего постановления возложить на заместителя министра Бондаренко С.С.

Министр Г.А. Лопаткин

Приложение
к постановлению
министерства
информационных
технологий и связи
Ростовской области
от «06» июня 2018 г. № 4

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых министерством информационных технологий и связи Ростовской области и аппаратом Правительства Ростовской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

Согласно аналитическому обоснованию определения актуальных угроз безопасности информации при их обработке в информационных системах министерства информационных технологий и связи Ростовской области и аппарата Правительства Ростовской области, актуальны следующие угрозы:

возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

угроза анализа криптографических алгоритмов и их реализации;

угроза внедрения кода или данных;

угроза воздействия на программы с высокими привилегиями;

угроза восстановления аутентификационной информации;

угроза выхода процесса за пределы виртуальной машины;

угроза длительного удержания вычислительных ресурсов пользователями;

угроза доступа к защищаемым файлам с использованием обходного пути;

угроза доступа к локальным файлам сервера при помощи URL;

угроза заражения DNS-кеша;

угроза избыточного выделения оперативной памяти;

угроза искажения XML-схемы;

угроза искажения вводимой и выводимой на периферийные устройства информации;

угроза использования альтернативных путей доступа к ресурсам;

угроза использования информации идентификации/аутентификации, заданной по умолчанию;

угроза использования механизмов авторизации для повышения привилегий;

угроза использования поддельных цифровых подписей BIOS;

угроза использования слабостей кодирования входных данных;

угроза использования слабостей протоколов сетевого/локального обмена данными;

угроза исследования механизмов работы программы;

угроза исследования приложения через отчёты об ошибках;

угроза исчерпания запаса ключей, необходимых для обновления BIOS;

угроза межсайтового скриптинга;

угроза межсайтовой подделки запроса;

угроза нарушения изоляции пользовательских данных внутри виртуальной машины;

угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;

угроза нарушения целостности данных кеша;

угроза неконтролируемого роста числа виртуальных машин;

угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;

угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера;

угроза некорректного использования функционала программного обеспечения;

угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

угроза неправомерных действий в каналах связи;

угроза несанкционированного восстановления удалённой защищаемой информации;

угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;

угроза несанкционированного доступа к аутентификационной информации;

угроза несанкционированного доступа к виртуальным каналам передачи;

угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети;

угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение;

угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;

угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин;

угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети;

угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;

угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;

угроза несанкционированного изменения аутентификационной информации;

угроза несанкционированного использования привилегированных функций BIOS;

угроза несанкционированного копирования защищаемой информации;
угроза несанкционированного редактирования реестра;
угроза несанкционированного создания учётной записи пользователя;
угроза несанкционированного удаления защищаемой информации;
угроза несанкционированного управления буфером;
угроза несанкционированного управления синхронизацией и состоянием;
угроза несанкционированного управления указателями;
угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
угроза обнаружения хостов;
угроза обхода некорректно настроенных механизмов аутентификации;
угроза опосредованного управления группой программ через совместно используемые данные;
угроза определения типов объектов защиты;
угроза определения топологии вычислительной сети;
угроза отключения контрольных датчиков;
угроза перебора всех настроек и параметров приложения;
угроза передачи данных по скрытым каналам;
угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;
угроза переполнения целочисленных переменных;
угроза перехвата вводимой и выводимой на периферийные устройства информации;
угроза перехвата данных, передаваемых по вычислительной сети;
угроза перехвата привилегированного потока;
угроза перехвата привилегированного процесса;
угроза перехвата управления гипервизором;
угроза перехвата управления средой виртуализации;
угроза повреждения системного реестра;
угроза повышения привилегий;
угроза подделки записей журнала регистрации событий;
угроза подмены действия пользователя путём обмана;
угроза подмены доверенного пользователя;
угроза подмены содержимого сетевых ресурсов;
угроза подмены субъекта сетевого доступа;
угроза получения предварительной информации об объекте защиты;
угроза получения сведений о владельце беспроводного устройства;
угроза преодоления физической защиты;
угроза приведения системы в состояние «отказ в обслуживании»;
угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
угроза пропуска проверки целостности программного обеспечения;
угроза сбоя обработки специальным образом изменённых файлов;
угроза удаления аутентификационной информации;
угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

угроза установки уязвимых версий обновления программного обеспечения BIOS;

угроза утраты вычислительных ресурсов;

угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

угроза форматирования носителей информации;

угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

угроза эксплуатации цифровой подписи программного кода;

угроза перехвата исключения/сигнала из привилегированного блока функций;

угроза неправомерного шифрования информации;

угроза скрытного включения вычислительного устройства в состав бот-сети;

угроза распространения «почтовых червей»;

угроза «фарминга»;

угроза «фишинга»;

угроза несанкционированного использования системных и сетевых утилит;

угроза несанкционированной модификации защищаемой информации;

угроза отказа подсистемы обеспечения температурного режима;

угроза несанкционированного изменения параметров настройки средств защиты информации;

угроза несанкционированного воздействия на средство защиты информации;

угроза маскирования действий вредоносного кода;

угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;

угроза внедрения вредоносного кода в дистрибутив программного обеспечения;

угроза использования уязвимых версий программного обеспечения;

угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;

угроза хищения аутентификационной информации из временных файлов cookie;

угроза скрытной регистрации вредоносной программной учетных записей администраторов;

угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов;

угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов;

угроза несанкционированной установки приложений на мобильные устройства.