

ГУБЕРНАТОР ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА - ЮГРЫ

ПОСТАНОВЛЕНИЕ от 11 декабря 2015 г. N 162

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в исполнительных органах государственной власти Ханты-Мансийского автономного округа - Югры

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" постановляю:

1. Утвердить прилагаемый перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в исполнительных органах государственной власти Ханты-Мансийского автономного округа - Югры при осуществлении ими соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки (далее - Перечень).

2. Руководителям исполнительных органов государственной власти Ханты-Мансийского автономного округа - Югры, а также подведомственных им учреждений до 30 апреля 2016 года разработать и утвердить с учетом Перечня частные модели угроз безопасности персональных данных при их обработке в информационных системах.

3. Рекомендовать органам местного самоуправления муниципальных образований Ханты-Мансийского автономного округа - Югры учитывать Перечень в процессе работ по обеспечению безопасности персональных данных.

Губернатор
Ханты-Мансийского
автономного округа - Югры
Н.В.КОМАРОВА

Приложение
к постановлению Губернатора
Ханты-Мансийского
автономного округа - Югры
от 11 декабря 2015 года N 162

ПЕРЕЧЕНЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫХ

**ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ЭКСПЛУАТИРУЕМЫХ В ИСПОЛНИТЕЛЬНЫХ
ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО
ОКРУГА - ЮГРЫ ПРИ ОСУЩЕСТВЛЕНИИ ИМИ СООТВЕТСТВУЮЩИХ ВИДОВ
ДЕЯТЕЛЬНОСТИ, С УЧЕТОМ СОДЕРЖАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ,
ХАРАКТЕРА И СПОСОБОВ ИХ ОБРАБОТКИ**

| № п/п | Наименование угрозы |
|-------|---|
| 1. | Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю |
| 1.1. | Угроза разглашения пользовательских имен и паролей |
| 1.2. | Просмотр (регистрация) персональных данных (далее - ПДн) с экранов дисплеев и других средств отображения графической, видео- и буквенно-цифровой информации |
| 1.3. | Угроза нарушения конфиденциальности информации посредством ее утечки в ходе ремонта, модификации и утилизации программно-аппаратных средств |
| 1.4. | Угроза несанкционированного доступа к ПДн |
| 1.5. | Угроза предоставления пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам информационных систем персональных данных (далее - ИСПДн) сверх объема, необходимого для работы |
| 1.6. | Угроза неумышленного (случайного) копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать копий документов с ПДн |
| 1.7. | Угроза преднамеренного копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать копий документов ПДн |
| 1.8. | Угроза неумышленной (случайной) модификации (искажения) доступных ПДн |
| 1.9. | Угроза преднамеренной модификации (искажения) доступных ПДн |
| 1.10. | Угроза неумышленного (случайного) добавления (фальсификации) ПДн |
| 1.11. | Угроза преднамеренного добавления (фальсификации) ПДн |
| 1.12. | Угроза неумышленного (случайного) уничтожения доступных ПДн (записей, файлов, форматирование диска) |
| 1.13. | Угроза преднамеренного уничтожения доступных ПДн (записей, файлов, форматирование диска) |
| 1.14. | Угроза использования для входа в систему чужих идентификаторов и паролей |
| 1.15. | Угроза изменения настроек и режимов работы программного обеспечения (далее - ПО), модификация ПО (удаление, искажение или подмена программных компонентов) |

| | |
|-------|---|
| | ИСПДн или средств защиты информации (далее - СЗИ)) |
| 1.16. | Угроза нарушения конфиденциальности информации посредством ее утечки по каналам передачи данных |
| 1.17. | Угроза нарушения конфиденциальности информации путем ее непосредственного сбора нарушителем в процессе эксплуатации ИСПДн |
| 1.18. | Угроза подключения к ИСПДн стороннего оборудования (компьютеров, дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи) |
| 1.19. | Угроза несанкционированного изменения конфигурационных файлов ПО (настроек экрана, сети, прикладных программ) |
| 1.20. | Угроза установки программных "шпионов" |
| 1.21. | Угроза использования оборудования, оставленного без присмотра, незаблокированных рабочих станций, использования чужих имен и паролей |
| 1.22. | Угроза применения специально созданных программ для повышения прав и привилегий |
| 1.23. | Угроза использования нетрадиционных каналов (например, стеганографии) для передачи ПДн |
| 1.24. | Угроза использования сторонних носителей данных |
| 1.25. | Угроза подключения к ИСПДн стороннего оборудования (компьютеров, смартфонов, телефонов, фотоаппаратов, видеокамер, флэш-дисков и иных устройств) |
| 1.26. | Угроза внедрения программных закладок, формирующих недеklarированные возможности программного обеспечения |
| 1.27. | Угроза преднамеренной установки вредоносных программ |
| 1.28. | Ошибки при разработке, развертывании и обслуживании программного обеспечения ИСПДн (в том числе СЗИ) |
| 1.29. | Преднамеренное внесение в программы при их разработке и развертывании вредоносных кодов (программных закладок) |
| 1.30. | Копирование информации с носителей ПДн |
| 1.31. | Хищение, утрата резервных копий носителей ПДн |
| 1.32. | Нарушение порядка резервного копирования ПДн |
| 1.33. | Угроза передачи ПДн по открытым сетям связи за пределы контролируемой зоны |
| 1.34. | Угроза использования программ-анализаторов пакетов (снифферов) для перехвата ПДн, в т.ч. для перехвата идентификаторов и паролей удаленного доступа |

| | |
|-------|---|
| 1.35. | Угроза пассивного сбора информации об объектах сети |
| 1.36. | Угроза частичного или полного исчерпания ресурсов |
| 1.37. | Угроза использования ошибок в программном обеспечении |
| 1.38. | Угроза активизации распространяемых злоумышленниками файлов при случайном обращении к ним пользователя |
| 1.39. | Угроза использования возможностей удаленного управления системой |
| 1.40. | Угроза нарушения работоспособности технических средств |
| 1.41. | Утеря или кража оборудования ИСПДн (в том числе резервных носителей информации) |
| 1.42. | Доступ к информации ИСПДн вследствие списания (утилизации) ее носителей, содержащих ПДн |
| 1.43 | Угрозы безопасности информации, размещенные на официальном сайте Федеральной службы по техническому и экспортному контролю (http://bdu.fstec.ru) |
| 2. | Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации |
| 2.1. | Непредумышленное искажение или удаление программных компонентов ИСПДн |
| 2.2. | Внедрение и использование неучтенных программ |
| 2.3. | Игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации |
| 2.4. | Нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности: ключевой, парольной и аутентифицирующей информации) |
| 2.5. | Предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований |
| 2.6. | Несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа |
| 2.7. | Внесение негативных функциональных возможностей в технические и программные компоненты криптосредства и среды функционирования (далее - СФ), в том числе с использованием вредоносных программ (компьютерные вирусы и т.д.) |
| 2.8. | Проведение атаки при нахождении в пределах контролируемой зоны |

| | |
|-------|---|
| 2.9. | Проведение атак на этапе эксплуатации средств криптографической защиты информации (далее - СКЗИ) на следующие объекты: - документацию на СКЗИ и СФ; - 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 СФ |
| 2.10. | 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 |
| 2.11. | Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |
| 2.12. | Физический доступ к СВТ, на которых реализованы СКЗИ и СФ |
| 2.13. | Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |
| 2.14. | Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО |
| 2.15. | 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 |
| 2.16. | Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ |
| 2.17. | Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО |
| 2.18. | Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ |

| | |
|-------|--|
| 2.19. | Возможность воздействовать на любые компоненты СКЗИ и СФ |
|-------|--|
