ПРАВИТЕЛЬСТВО РОСТОВСКОЙ ОБЛАСТИ

УПРАВЛЕНИЕ ЗАПИСИ АКТОВ ГРАЖДАНСКОГО СОСТОЯНИЯ (УПРАВЛЕНИЕ ЗАГС РОСТОВСКОЙ ОБЛАСТИ)

П О С Т А Н О В Л Е Н И Е

от 04.10.2017 № 3

г. Ростов-на-Дону

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных управления записи актов гражданского состояния Ростовской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», управление записи актов гражданского состояния Ростовской области **п о с т а н о в л я е т :**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных управления записи актов гражданского состояния Ростовской области и органах ЗАГС Ростовской области согласно приложению.

2. Специалисту отдела архивной работы, автоматизации и информатики, ответственному за обеспечение защиты информации при эксплуатации информационных систем персональных данных управления записи актов гражданского состояния Ростовской области и обработке персональных данных, руководствоваться настоящим постановлением.

3. Рекомендовать отделам ЗАГС муниципальных образований Ростовской области при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при регистрации актов гражданского состояния, использовать настоящее постановление.

4. Настоящее постановление вступает в силу со дня его официального опубликования.

5. Контроль за выполнением настоящего постановления возложить на начальника отдела архивной работы, автоматизации и информатики.

Начальник управления ЗАГС
Ростовской области — Г.Г. Слюсарева

Постановление вносит отдел архивной работы, автоматизации и информатики

Приложение
к постановлению
управления ЗАГС
Ростовской области
от 04.10.2017 № 3

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных управления записи актов гражданского состояния Ростовской области

1. Угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю Российской Федерации

1.1. Для информационной системы персональных данных управления ЗАГС Ростовской области:

1.1.1. угроза аппаратного сброса пароля BIOS;

1.1.2. угроза внедрения кода или данных;

1.1.3. угроза восстановления аутентификационной информации;

1.1.4. угроза восстановления предыдущей уязвимой версии BIOS;

1.1.5. угроза деструктивного изменения конфигурации/среды окружения программ;

1.1.6. угроза деструктивного использования декларированного функционала BIOS;

1.1.7. угроза длительного удержания вычислительных ресурсов пользователями;

1.1.8. угроза доступа к защищаемым файлам с использованием обходного пути;

1.1.9. угроза доступа/перехвата/изменения HTTP cookies;

1.1.10. угроза загрузки нештатной операционной системы;

1.1.11. угроза заражения DNS-кеша;

1.1.12. угроза избыточного выделения оперативной памяти;

1.1.13. угроза изменения компонентов системы;

1.1.14. угроза искажения вводимой и выводимой на периферийные устройства информации;

1.1.15. угроза использования альтернативных путей доступа к ресурсам;

1.1.16. угроза использования информации идентификации/аутентификации, заданной по умолчанию;

1.1.17. угроза использования механизмов авторизации для повышения привилегий;

1.1.18. угроза использования слабостей протоколов сетевого/локального обмена данными;

1.1.19. угроза межсайтового скриптинга;

1.1.20. угроза нарушения изоляции среды исполнения BIOS;

1.1.21. угроза нарушения целостности данных кеша;

1.1.22. угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;

1.1.23. угроза невозможности управления правами пользователей BIOS;

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

1.1.25. угроза неправомерного ознакомления с защищаемой информацией;

1.1.26. угроза неправомерных действий в каналах связи;

1.1.27. угроза несанкционированного восстановления удалённой защищаемой информации;

1.1.28. угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

1.1.29. угроза несанкционированного доступа к аутентификационной информации;

1.1.30. угроза несанкционированного изменения аутентификационной информации;

1.1.31. угроза несанкционированного использования привилегированных функций BIOS;

1.1.32. угроза несанкционированного копирования защищаемой информации;

1.1.33. угроза несанкционированного редактирования реестра;

1.1.34. угроза несанкционированного создания учётной записи пользователя;

1.1.35. угроза несанкционированного удаления защищаемой информации;

1.1.36. угроза несанкционированного управления буфером;

1.1.37. угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

1.1.38. угроза обнаружения хостов;

1.1.39. угроза обхода некорректно настроенных механизмов аутентификации;

1.1.40. угроза определения типов объектов защиты;

1.1.41. угроза определения топологии вычислительной сети;

1.1.42. угроза отключения контрольных датчиков;

1.1.43. угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;

1.1.44. угроза перехвата вводимой и выводимой на периферийные устройства информации;

1.1.45. угроза перехвата данных, передаваемых по вычислительной сети;

1.1.46. угроза повреждения системного реестра;

1.1.47. угроза подбора пароля BIOS;

1.1.48. угроза подделки записей журнала регистрации событий;

1.1.49. угроза подмены доверенного пользователя;

1.1.50. угроза подмены резервной копии программного обеспечения BIOS;

1.1.51. угроза подмены содержимого сетевых ресурсов;

1.1.52. угроза приведения системы в состояние «отказ в обслуживании»;

1.1.53. угроза программного сброса пароля BIOS;

1.1.54. угроза пропуска проверки целостности программного обеспечения;

1.1.55. угроза удаления аутентификационной информации;

1.1.56. угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

1.1.57. угроза утраты вычислительных ресурсов;

1.1.58. угроза утраты носителей информации;

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

1.1.60. угроза форматирования носителей информации;

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

1.1.62. угроза эксплуатации цифровой подписи программного кода;

1.1.63. угроза заражения компьютера при посещении неблагонадёжных сайтов;

1.1.64. угроза «кражи» учётной записи доступа к сетевым сервисам;

1.1.65. угроза неправомерного шифрования информации;

1.1.66. угроза скрытного включения вычислительного устройства в состав бот-сети;

1.1.67. угроза распространения «почтовых червей»;

1.1.68. угроза «фарминга»;

1.1.69. угроза «фишинга»;

1.1.70. угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;

1.1.71. угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;

1.1.72. угроза несанкционированного использования системных и сетевых утилит;

1.1.73. угроза несанкционированной модификации защищаемой информации;

1.1.74. угроза отказа подсистемы обеспечения температурного режима;

1.1.75. угроза физического устаревания аппаратных компонентов;

1.1.76. угроза несанкционированного изменения параметров настройки средств защиты информации;

1.1.77. угроза внедрения вредоносного кода через рекламу, сервисы и контент;

1.1.78. угроза внедрения вредоносного кода в дистрибутив программного обеспечения;

1.1.79. угроза использования уязвимых версий программного обеспечения.

1.2. Для информационной системы персональных данных отдела архивной работы, автоматизации и информатики управления ЗАГС Ростовской области:

1.2.1. угроза анализа криптографических алгоритмов и их реализации;

1.2.2. угроза аппаратного сброса пароля BIOS;

1.2.3. угроза внедрения вредоносного кода в BIOS;

1.2.4. угроза внедрения кода или данных;

1.2.5. угроза воздействия на программы с высокими привилегиями;

1.2.6. угроза восстановления аутентификационной информации;

1.2.7. угроза восстановления предыдущей уязвимой версии BIOS;

1.2.8. угроза выхода процесса за пределы виртуальной машины;

1.2.9. угроза деструктивного изменения конфигурации/среды окружения программ;

1.2.10. угроза деструктивного использования декларированного функционала BIOS;

1.2.11. угроза длительного удержания вычислительных ресурсов пользователями;

1.2.12. угроза доступа к защищаемым файлам с использованием обходного пути;

1.2.13. угроза доступа к локальным файлам сервера при помощи URL;

1.2.14. угроза доступа/перехвата/изменения HTTP cookies;

1.2.15. угроза загрузки нештатной операционной системы;

1.2.16. угроза заражения DNS-кеша;

1.2.17. угроза несанкционированного редактирования реестра;

1.2.18. угроза заражения компьютера при посещении неблагонадёжных сайтов;

1.2.19. угроза избыточного выделения оперативной памяти;

1.2.20. угроза изменения компонентов системы;

1.2.21. угроза изменения режимов работы аппаратных элементов компьютера;

1.2.22. угроза изменения системных и глобальных переменных;

1.2.23. угроза искажения XML-схемы;

1.2.24. угроза искажения вводимой и выводимой на периферийные устройства информации;

1.2.25. угроза использования альтернативных путей доступа к ресурсам;

1.2.26. угроза использования информации идентификации/аутентификации, заданной по умолчанию;

1.2.27. угроза использования механизмов авторизации для повышения привилегий;

1.2.28. угроза использования поддельных цифровых подписей BIOS;

1.2.29. угроза использования слабостей кодирования входных данных;

1.2.30. угроза использования слабостей протоколов сетевого/локального обмена данными;

1.2.31. угроза использования слабых криптографических алгоритмов BIOS;

1.2.32. угроза исследования механизмов работы программы;

1.2.33. угроза исследования приложения через отчёты об ошибках;

1.2.34. угроза исчерпания запаса ключей, необходимых для обновления BIOS;

1.2.35. угроза «кражи» учётной записи доступа к сетевым сервисам;

1.2.36. угроза нарушения изоляции пользовательских данных внутри виртуальной машины;

1.2.37. угроза нарушения изоляции среды исполнения BIOS;

1.2.38. угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

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

1.2.40. угроза нарушения целостности данных кеша;

1.2.41. угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;

1.2.42. угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения;

1.2.43. угроза невозможности управления правами пользователей BIOS;

1.2.44. угроза скрытного включения вычислительного устройства в состав бот-сети;

1.2.45. угроза распространения «почтовых червей»;

1.2.46. угроза неконтролируемого роста числа виртуальных машин;

1.2.47. угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;

1.2.48. угроза некорректного задания структуры данных транзакции;

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

1.2.50. угроза некорректного использования функционала программного обеспечения;

1.2.51. угроза «фарминга»;

1.2.52. угроза «фишинга»;

1.2.53. угроза внедрения вредоносного кода через рекламу, сервисы и контент;

1.2.54. угроза неправомерного ознакомления с защищаемой информацией;

1.2.55. угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

1.2.56. угроза неправомерных действий в каналах связи;

1.2.57. угроза внедрения вредоносного кода за счет посещения зараженных сайтов в информационно-телекоммуникационной сети Интернет;

1.2.58. угроза несанкционированного восстановления удалённой защищаемой информации;

1.2.59. угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

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

1.2.61. угроза несанкционированного доступа к аутентификационной информации;

1.2.62. угроза несанкционированного доступа к виртуальным каналам передачи;

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

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

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

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

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

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

1.2.69. угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;

1.2.70. угроза несанкционированного изменения аутентификационной информации;

1.2.71. угроза несанкционированного использования привилегированных функций BIOS;

1.2.72. угроза несанкционированного копирования защищаемой информации;

1.2.73. угроза несанкционированного создания учётной записи пользователя;

1.2.74. угроза несанкционированного удаления защищаемой информации;

1.2.75. угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам;

1.2.76. угроза несанкционированного управления буфером;

1.2.77. угроза несанкционированного управления синхронизацией и состоянием;

1.2.78. угроза несанкционированного управления указателями;

1.2.79. угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

1.2.80. угроза обнаружения хостов;

1.2.81. угроза обхода некорректно настроенных механизмов аутентификации;

1.2.82. угроза опосредованного управления группой программ через совместно используемые данные;

1.2.83. угроза определения типов объектов защиты;

1.2.84. угроза определения топологии вычислительной сети;

1.2.85. угроза отключения контрольных датчиков;

1.2.86. угроза ошибки обновления гипервизора;

1.2.87. угроза перебора всех настроек и параметров приложения;

1.2.88. угроза передачи данных по скрытым каналам;

1.2.89. угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;

1.2.90. угроза переполнения целочисленных переменных;

1.2.91. угроза перехвата вводимой и выводимой на периферийные устройства информации;

1.2.92. угроза перехвата данных, передаваемых по вычислительной сети;

1.2.93. угроза перехвата привилегированного потока;

1.2.94. угроза перехвата привилегированного процесса;

1.2.95. угроза перехвата управления гипервизором;

1.2.96. угроза перехвата управления средой виртуализации;

1.2.97. угроза повреждения системного реестра;

1.2.98. угроза повышения привилегий;

1.2.99. угроза подбора пароля BIOS;

1.2.100. угроза подделки записей журнала регистрации событий;

1.2.101. угроза подмены действия пользователя путём обмана;

1.2.102. угроза подмены доверенного пользователя;

1.2.103. угроза подмены резервной копии программного обеспечения BIOS;

1.2.104. угроза подмены содержимого сетевых ресурсов;

1.2.105. угроза подмены субъекта сетевого доступа;

1.2.106. угроза получения предварительной информации об объекте защиты;

1.2.107. угроза преодоления физической защиты;

1.2.108. угроза приведения системы в состояние «отказ в обслуживании»;

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

1.2.110. угроза программного сброса пароля BIOS;

1.2.111. угроза пропуска проверки целостности программного обеспечения;

1.2.112. угроза сбоя обработки специальным образом изменённых файлов;

1.2.113. угроза сбоя процесса обновления BIOS;

1.2.114. угроза удаления аутентификационной информации;

1.2.115. угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

1.2.116. угроза установки уязвимых версий обновления программного обеспечения BIOS;

1.2.117. угроза утраты вычислительных ресурсов;

1.2.118. угроза утраты носителей информации;

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

1.2.120. угроза форматирования носителей информации;

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

1.2.122. угроза эксплуатации цифровой подписи программного кода;

1.2.123. угроза перехвата исключения/сигнала из привилегированного блока функций;

1.2.124. угроза включения в проект не достоверно испытанных компонентов;

1.2.125. угроза внедрения системной избыточности;

1.2.126. угроза наличия механизмов разработчика;

1.2.127. угроза неправомерного шифрования информации;

1.2.128. угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;

1.2.129. угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;

1.2.130. угроза несанкционированного использования системных и сетевых утилит;

1.2.131. угроза несанкционированной модификации защищаемой информации;

1.2.132. угроза отказа подсистемы обеспечения температурного режима;

1.2.133. угроза физического устаревания аппаратных компонентов;

1.2.134. угроза несанкционированного изменения параметров настройки средств защиты информации;

1.2.135. угроза несанкционированного воздействия на средство защиты информации;

1.2.136. угроза подмены программного обеспечения;

1.2.137. угроза маскирования действий вредоносного кода;

1.2.138. угроза внедрения вредоносного кода в дистрибутив программного обеспечения;

1.2.139. угроза использования уязвимых версий программного обеспечения;

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

2. Угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации

2.1. Для информационной системы персональных данных управления ЗАГС Ростовской области:

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

2.1.2. возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы средства криптографической защиты информации (далее – СКЗИ) и среда их функционирования (далее – СФ);

2.1.3. 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 средства вычислительной техники, на которых реализованы СКЗИ и СФ.

2.2. Для информационной системы персональных данных отдела архивной работы, автоматизации и информатики управления ЗАГС Ростовской области:

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

2.2.2. возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы средства криптографической защиты информации (далее – СКЗИ) и среда их функционирования (далее – СФ);

2.2.3. 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 средства вычислительной техники, на которых реализованы СКЗИ и СФ.

Начальник отдела архивной работы,
автоматизации и информатики М.В. Хлебников