ПРАВИТЕЛЬСТВО ТУЛЬСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 21.06.2018 № 241

О внесении изменений в постановление правительства Тульской области от 29.10.2015 № 504

С целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Тульской области, в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», на основании статьи 48 Устава (Основного Закона) Тульской области правительство Тульской области ПОСТАНОВЛЯЕТ:

1. Утвердить изменения, которые вносятся в постановление правительства Тульской области от 29.10.2015 № 504 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях», согласно приложению.

2. Постановление вступает в силу со дня официального опубликования.

Первый заместитель Губернатора Тульской области – председатель правительства Тульской области Управление по делопроизводству и работе с обращениями граждан **Ю.М. Андрианов**

103654 707206

Приложение
к постановлению правительства
Тульской области

от 21.06.2018 № 241

ИЗМЕНЕНИЯ,
которые вносятся в постановление правительства Тульской области от 29.10.2015 № 504 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях»

1. В названии, преамбуле и пункте 1 постановления текст «в органах исполнительной власти Тульской области, аппарате правительства Тульской области и подведомственных им учреждениях и организациях» заменить текстом «(государственных информационных системах) Тульской области».

2. Приложение к постановлению изложить в новой редакции:

«Приложение
к постановлению правительства
Тульской области

от 29.10.2015 № 504

УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ,
актуальные при обработке персональных данных в информационных системах персональных данных (государственных информационных системах) Тульской области

1. Проведение атаки при нахождении в пределах контролируемой зоны.

2. Проведение атак на этапе эксплуатации средств криптографической защиты информации на следующие объекты:

документацию на средства криптографической защиты информации и компоненты среды функционирования средств криптографической защиты информации;

помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее –

средства вычислительной техники), на которых реализованы средства криптографической защиты информации и среда функционирования.

3. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

сведений о физических мерах защиты объектов, в которых размещены ресурсы региональных информационных систем правительства Тульской области (далее – РИС ТО);

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы РИС ТО;

сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования.

4. Использование штатных средств РИС ТО, ограниченное мерами, реализованными в информационной системе, в которой используется средства криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий.

5. Физический доступ к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования.

6. Возможность воздействовать на аппаратные компоненты средства криптографической защиты информации и среда функционирования, ограниченная мерами, реализованными в информационной системе, в которой используются средства криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий.

7. УБИ(*). 003. Угроза анализа криптографических алгоритмов и их реализации.

8. УБИ. 004. Угроза аппаратного сброса пароля BIOS.

9. УБИ. 005. Угроза внедрения вредоносного кода в BIOS.

10. УБИ. 006. Угроза внедрения кода или данных.

11. УБИ. 007. Угроза воздействия на программы с высокими привилегиями.

12. УБИ. 008. Угроза восстановления аутентификационной информации.

13. УБИ. 010. Угроза выхода процесса за пределы виртуальной машины.

14. УБИ. 012. Угроза деструктивного изменения конфигурации/среды окружения программ.

15. УБИ. 013. Угроза деструктивного использования декларированного функционала BIOS.

16. УБИ. 014. Угроза длительного удержания вычислительных ресурсов пользователями.

17. УБИ. 015. Угроза доступа к защищаемым файлам с использованием обходного пути.

18. УБИ. 016. Угроза доступа к локальным файлам сервера при помощи URL.

19. УБИ. 017. Угроза доступа/перехвата/изменения HTTP cookies.

20. УБИ. 018. Угроза загрузки нештатной операционной системы.

21. УБИ. 019. Угроза заражения DNS-кеша.

22. УБИ. 022. Угроза избыточного выделения оперативной памяти.

23. УБИ. 023. Угроза изменения компонентов системы.

24. УБИ. 026. Угроза искажения XML-схемы.

25. УБИ. 028. Угроза использования альтернативных путей доступа к ресурсам.

26. УБИ. 030. Угроза использования информации идентификации/аутентификации, заданной по умолчанию.

27. УБИ. 031. Угроза использования механизмов авторизации для повышения привилегий.

28. УБИ. 032. Угроза использования поддельных цифровых подписей BIOS.

29. УБИ. 033. Угроза использования слабостей кодирования входных данных.

30. УБИ. 034. Угроза использования слабостей протоколов сетевого/локального обмена данными.

31. УБИ. 036. Угроза исследования механизмов работы программы.

32. УБИ. 037. Угроза исследования приложения через отчёты об ошибках.

33. УБИ. 041. Угроза межсайтового скриптинга.

34. УБИ. 042. Угроза межсайтовой подделки запроса.

35. УБИ. 044. Угроза нарушения изоляции пользовательских данных внутри виртуальной машины.

36. УБИ. 045. Угроза нарушения изоляции среды исполнения BIOS.

37. УБИ. 046. Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия.

38. УБИ. 048. Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин.

39. УБИ. 049. Угроза нарушения целостности данных кеша.

40. УБИ. 053. Угроза невозможности управления правами пользователей BIOS.

41. УБИ. 059. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов.

42. УБИ. 061. Угроза некорректного задания структуры данных транзакции.

43. УБИ. 062. Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера.

44. УБИ. 063. Угроза некорректного использования функционала программного обеспечения.

45. УБИ. 067. Угроза неправомерного ознакомления с защищаемой информацией.

46. УБИ. 068. Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.

47. УБИ. 069. Угроза неправомерных действий в каналах связи.

48. УБИ. 071. Угроза несанкционированного восстановления удалённой защищаемой информации.

49. УБИ. 072. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.

50. УБИ. 073. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.

51. УБИ. 074. Угроза несанкционированного доступа к аутентификационной информации.

52. УБИ. 075. Угроза несанкционированного доступа к виртуальным каналам передачи.

53. УБИ. 076. Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети.

54. УБИ. 077. Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение.

55. УБИ. 078. Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети.

56. УБИ. 079. Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин.

57. УБИ. 080. Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети.

58. УБИ. 084. Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети.

59. УБИ. 085. Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации.

60. УБИ. 086. Угроза несанкционированного изменения аутентификационной информации.

61. УБИ. 088. Угроза несанкционированного копирования защищаемой информации.

62. УБИ. 089. Угроза несанкционированного редактирования реестра.

63. УБИ. 090. Угроза несанкционированного создания учётной записи пользователя.

64. УБИ. 091. Угроза несанкционированного удаления защищаемой информации.

65. УБИ. 093. Угроза несанкционированного управления буфером.

66. УБИ. 094. Угроза несанкционированного управления синхронизацией и состоянием.

67. УБИ. 095. Угроза несанкционированного управления указателями.

68. УБИ. 098. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.

69. УБИ. 099. Угроза обнаружения хостов.

70. УБИ. 100. Угроза обхода некорректно настроенных механизмов аутентификации.

71. УБИ. 102. Угроза опосредованного управления группой программ через совместно используемые данные.

72. УБИ. 103. Угроза определения типов объектов защиты.

73. УБИ. 104. Угроза определения топологии вычислительной сети.

74. УБИ. 109. Угроза перебора всех настроек и параметров приложения.

75. УБИ. 111. Угроза передачи данных по скрытым каналам.

76. УБИ. 113. Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.

77. УБИ. 114. Угроза переполнения целочисленных переменных.

78. УБИ. 115. Угроза перехвата вводимой и выводимой на периферийные устройства информации.

79. УБИ. 116. Угроза перехвата данных, передаваемых по вычислительной сети.

80. УБИ. 117. Угроза перехвата привилегированного потока.

81. УБИ. 118. Угроза перехвата привилегированного процесса.

82. УБИ. 119. Угроза перехвата управления гипервизором.

83. УБИ. 120. Угроза перехвата управления средой виртуализации.

84. УБИ. 121. Угроза повреждения системного реестра.

85. УБИ. 122. Угроза повышения привилегий.

86. УБИ. 123. Угроза подбора пароля BIOS.

87. УБИ. 124. Угроза подделки записей журнала регистрации событий.

88. УБИ. 127. Угроза подмены действия пользователя путём обмана.

89. УБИ. 128. Угроза подмены доверенного пользователя.

90. УБИ. 130. Угроза подмены содержимого сетевых ресурсов.

91. УБИ. 131. Угроза подмены субъекта сетевого доступа.

92. УБИ. 132. Угроза получения предварительной информации об объекте защиты.

93. УБИ. 139. Угроза преодоления физической защиты.

94. УБИ. 140. Угроза приведения системы в состояние «отказ в обслуживании».

95. УБИ. 143. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.

96. УБИ. 144. Угроза программного сброса пароля BIOS.

97. УБИ. 145. Угроза пропуска проверки целостности программного обеспечения.

98. УБИ. 149. Угроза сбоя обработки специальным образом изменённых файлов.

99. УБИ. 151. Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL.

100. УБИ. 152. Угроза удаления аутентификационной информации.

101. УБИ. 153. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.

102. УБИ. 155. Угроза утраты вычислительных ресурсов.

103. УБИ. 156. Угроза утраты носителей информации.

104. УБИ. 157. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.

105. УБИ. 158. Угроза форматирования носителей информации.

106. УБИ. 159. Угроза «форсированного веб-браузинга».

107. УБИ. 160. Угроза хищения средств хранения, обработки и (или) ввода/вывода/ передачи информации.

108. УБИ. 162. Угроза эксплуатации цифровой подписи программного кода.

109. УБИ. 163. Угроза перехвата исключения/сигнала из привилегированного блока функций.

110. УБИ. 165. Угроза включения в проект не достоверно испытанных компонентов.

111. УБИ. 166. Угроза внедрения системной избыточности.

112. УБИ. 167. Угроза заражения компьютера при посещении неблагонадёжных сайтов.

113. УБИ. 168. Угроза «кражи» учётной записи доступа к сетевым сервисам.

114. УБИ. 169. Угроза наличия механизмов разработчика.

115. УБИ. 170. Угроза неправомерного шифрования информации.

116. УБИ. 171. Угроза скрытного включения вычислительного устройства в состав бот-сети.

117. УБИ. 172. Угроза распространения «почтовых червей».

118. УБИ. 173. Угроза «спама» веб-сервера.

119. УБИ. 174. Угроза «фарминга».

120. УБИ. 175. Угроза «фишинга».

121. УБИ. 177. Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью.

122. УБИ. 178. Угроза несанкционированного использования системных и сетевых утилит.

123. УБИ. 179. Угроза несанкционированной модификации защищаемой информации.

124. УБИ. 185. Угроза несанкционированного изменения параметров настройки средств защиты информации.

125. УБИ. 186. Угроза внедрения вредоносного кода через рекламу, сервисы и контент.

126. УБИ. 187. Угроза несанкционированного воздействия на средство защиты информации.

127. УБИ. 188. Угроза подмены программного обеспечения.

128. УБИ. 189. Угроза маскирования действий вредоносного кода.

129. УБИ. 190. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет.

130. УБИ. 191. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

131. УБИ. 192. Угроза использования уязвимых версий программного обеспечения.

132. УБИ. 193. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика.

133. УБИ. 194. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы.

134. УБИ.197: Угроза хищения аутентификационной информации из временных файлов cookie.

135. УБИ.198: Угроза скрытной регистрации вредоносной программой учетных записей администраторов.

136. УБИ.201: Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере.

137. УБИ.205: Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты.

138. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

*УБИ – угроза безопасности информации из банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (http://bdu.fstec.ru).».