ПРАВИТЕЛЬСТВО СТАВРОПОЛЬСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

10 января 2019 г. г.Ставрополь № 4-п

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности Правительства Ставропольского края

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» и с учетом содержания персональных данных, обрабатываемых в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности Правительства Ставропольского края, характера и способов их обработки Правительство Ставропольского края

ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности Правительства Ставропольского края, согласно приложению к настоящему постановлению (далее – актуальные угрозы безопасности).

2. Органам исполнительной власти Ставропольского края и иным государственным органам Ставропольского края, образованным Губернатором Ставропольского края, Правительством Ставропольского края, определить актуальные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности.

3. Государственному казенному учреждению Ставропольского края «Краевой центр информационных технологий» в течение 60 рабочих дней со дня принятия настоящего постановления разработать частные модели угроз с учетом раздела 3 Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432.

4. Контроль за выполнением настоящего постановления возложить на заместителя председателя Правительства Ставропольского края, руководителя аппарата Правительства Ставропольского края Гладкова В.В.

5. Настоящее постановление вступает в силу со дня его принятия.

Губернатор
Ставропольского края В.В.Владимиров

Приложение

к постановлению Правительства
Ставропольского края
от 10 января 2019 г. № 4-п

УГРОЗЫ

безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых для осуществления деятельности Правительства Ставропольского края

I. Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых для осуществления деятельности Правительства Ставропольского края (далее соответственно – актуальные угрозы безопасности, информационные системы), разработаны в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» с учётом содержания персональных данных, обрабатываемых в информационных системах, характера и способов их обработки.

2. Под актуальными угрозами безопасности понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

3. Для определения актуальных угроз безопасности из систематизированного перечня угроз безопасности, содержащегося в Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г., выбираются только те угрозы, которые являются актуальными для информационной системы в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Заместителем директора Федеральной службы по техническому и экспортному контролю 14 февраля 2008 г.

4. Актуальные угрозы безопасности уточняются и дополняются по мере выявления новых источников угроз безопасности персональных данных, развития способов и средств реализации угроз безопасности персональных данных в информационных системах.

5. В Правительстве Ставропольского края создаются и эксплуатируются информационные системы, в которых могут обрабатываться персональные данные.

Такие информационные системы характеризуются тем, что в качестве объектов информатизации выступают локальные автоматизированные рабочие места или автоматизированные рабочие места, подключенные к локальным вычислительным сетям, объединенные в объектовые информационные системы либо являющиеся сегментами информационных систем сторонних операторов, имеющие или не имеющие подключение к сетям общего пользования и (или) сетям международного информационного обмена.

6. Ввод персональных данных в информационные системы осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные могут выводиться из информационной системы в электронном виде или на бумажных носителях.

7. Состав персональных данных, обрабатываемых с использованием информационных систем, определяется Губернатором Ставропольского края.

8. В Правительстве Ставропольского края создаются и эксплуатируются информационные системы, которые могут быть однотипными или разноплановыми с информационными системами иных органов исполнительной власти Ставропольского края, государственных органов Ставропольского края, образованных Губернатором Ставропольского края, Правительством Ставропольского края (далее – государственные органы).

9. Однотипные информационные системы предназначены для обеспечения типовой деятельности Правительства Ставропольского края, органов исполнительной власти Ставропольского края, государственных органов и используются для автоматизации их деятельности в рамках исполнения ими типовых полномочий, предусмотренных нормативными правовыми актами.

Контролируемой зоной однотипных информационных систем является здание Правительства Ставропольского края.

В пределах контролируемой зоны однотипных информационных систем находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование таких информационных систем.

Вне контролируемой зоны однотипных информационных систем находятся линии передачи данных и телекоммуникационное оборудование, ис-

пользуемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

Помещения, в которых размещаются однотипные информационные системы, должны быть оборудованы средствами контроля доступа, а также должна осуществляться их физическая охрана.

Здание Правительства Ставропольского края должно быть оборудовано системами видеонаблюдения.

Однотипные информационные системы обладают следующими особенностями:

использование стандартных (унифицированных) технических средств обработки информации;

использование типового программного обеспечения;

наличие незначительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

дублирование информации, содержащей персональные данные, на бумажных носителях и машинных носителях информации;

наличие незначительных негативных последствий для субъектов персональных данных при реализации угроз безопасности;

применение жесткой регламентации процедур взаимодействия со сторонними организациями (банками, пенсионными, страховыми и налоговыми органами, органами статистики).

10. Разноплановые информационные системы характеризуются тем, что в качестве объектов информатизации выступают локальные или распределенные информационные системы регионального масштаба, подключенные к сетям общего пользования и (или) сетям международного информационного обмена.

Разноплановые информационные системы обладают следующими особенностями:

использование широкой номенклатуры технических средств получения, отображения и обработки информации;

использование специального программного обеспечения;

наличие значительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

построение информационной системы на базе распределенной региональной вычислительной сети со сложной архитектурой;

наличие подключений к сетям связи общего пользования и (или) международного информационного обмена;

использование разнообразной телекоммуникационной инфраструктуры, принадлежащей различным операторам связи;

широкое применение средств защиты информации, включая сертифицированные средства криптографической защиты информации;

сложность дублирования больших массивов информации, содержащей персональные данные, на бумажных носителях и машинных носителях информации;

значительные негативные последствия при реализации угроз безопасности;

недостаточной квалификацией пользователей и персонала, обслуживающего разноплановые информационные системы и средства защиты информации.

II. Однотипные информационные системы

11. К однотипным информационным системам относятся:

1) информационные системы управления персоналом, предназначенные для обработки персональных данных, необходимых для предоставления информации в пенсионные органы, систему обязательного медицинского страхования, для персонального кадрового учета, управления кадровым резервом, проведения аттестации, повышения квалификации и для других целей, связанных с управлением персоналом;

2) информационная система управления финансами, предназначенная для обработки персональных данных, необходимых для бухгалтерского и управленческого финансового учета, предоставления информации в пенсионные и налоговые органы, а также для других целей, связанных с обеспечением финансовой деятельности Правительства Ставропольского края.

12. Оператором информационных систем управления персоналом и информационной системы управления финансами выступает Правительство Ставропольского края.

13. Информационные системы управления персоналом и информационная система управления финансами являются локальными и размещаются в здании Правительства Ставропольского края.

14. Для обеспечения конфиденциальности, целостности, доступности и подлинности персональных данных, обрабатываемых в информационных системах управления персоналом и информационной системе управления финансами, используются сертифицированные средства защиты информации.

15. Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена в информационных системах управления персоналом и информационной системе управления финансами не осуществляется, средства криптографической защиты информации не используются.

III. Разноплановые информационные системы

16. К разноплановым информационным системам относится сегмент информационной системы электронного делопроизводства и документооборота, предназначенной для автоматизации делопроизводства, служебной переписки, архивной деятельности, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам.

17. В сегменте информационной системы электронного делопроизводства и документооборота ведется обработка персональных данных граждан, обратившихся в Правительство Ставропольского края.

18. Для обеспечения конфиденциальности, целостности, доступности и подлинности персональных данных, обрабатываемых в информационной системе электронного делопроизводства и документооборота используются сертифицированные средства защиты информации.

19. Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена в информационной системе электронного делопроизводства и документооборота осуществляется с использованием сертифицированных средств криптографической защиты информации.

20. Информационная система электронного делопроизводства и документооборота является распределенной.

21. Оператором информационной системы электронного делопроизводства и документооборота является государственное казенное учреждение Ставропольского края «Краевой центр информационных технологий».

22. В информационной системе электронного делопроизводства и документооборота существуют актуальные угрозы безопасности, которые могут быть нейтрализованы только с помощью средств криптографической защиты информации, так как осуществляется передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий в отношении такой информации.

23. В информационной системе электронного делопроизводства и документооборота не используются отчуждаемые носители защищаемой информации, для которых несанкционированный доступ к хранимой на них информации не может быть исключен без использования криптографических методов и способов.

IV. Актуальные угрозы безопасности

24. Актуальными угрозами безопасности в однотипных информационных системах являются:

1) угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода (вывода) (BIOS), перехват управления загрузкой;

2) угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, с применением специальных программ для осуществления НСД;

3) угрозы внедрения вредоносных программ (локально);

4) угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;

5) угрозы сканирования, направленные на выявление типа операционной системы информационных систем, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений;

6) угрозы выявление паролей;

7) угрозы получения несанкционированного доступа путем подмены доверенного объекта;

8) угрозы типа «Отказ в обслуживании»;

9) угрозы удалённого запуска приложений;

10) угрозы внедрения по сети вредоносных программ;

11) УБИ.006. Угроза внедрения кода или данных;

12) УБИ.007. Угроза воздействия на программы с высокими привилегиями;

13) УБИ.008. Угроза восстановления аутентификационной информации;

14) УБИ.015. Угроза доступа к защищаемым файлам с использованием обходного пути;

15) УБИ.017. Угроза доступа, перехвата, изменения HTTP cookies;

16) УБИ.019. Угроза заражения DNS-кеша;

17) УБИ.023. Угроза изменения компонентов системы;

18) УБИ.028. Угроза использования альтернативных путей доступа к ресурсам;

19) УБИ.030. Угроза использования информации идентификации (аутентификации), заданной по умолчанию;

20) УБИ.031. Угроза использования механизмов авторизации для повышения привилегий;

21) УБИ.034. Угроза использования слабостей протоколов сетевого (локального) обмена данными;

22) УБИ.049. Угроза нарушения целостности данных кеша;

23) УБИ.062. Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера;

24) УБИ.063. Угроза некорректного использования функционала программного обеспечения;

25) УБИ.067. Угроза неправомерного ознакомления с защищаемой информацией;

26) УБИ.069. Угроза неправомерных действий в канал связи;

27) УБИ.071. Угроза несанкционированного восстановления удаленной защищаемой информации;

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

29) УБИ.074. Угроза несанкционированного доступа к аутентификационной информации;

30) УБИ.086. Угроза несанкционированного изменения аутентификационной информации;

31) УБИ.088. Угроза несанкционированного копирования защищаемой информации;

32) УБИ.089. Угроза несанкционированного редактирования реестра;

33) УБИ.090. Угроза несанкционированного создания учетной записи пользователя;

34) УБИ.091. Угроза несанкционированного удаления защищаемой информации;

35) УБИ.098. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

36) УБИ.099. Угроза обнаружения хостов;

37) УБИ.100. Угроза обхода некорректно настроенных механизмов аутентификации;

38) УБИ.103. Угроза определения типов объектов защиты;

39) УБИ.104. Угроза определения топологии вычислительной сети;

40) УБИ.116. Угроза перехвата данных, передаваемых по вычислительной сети;

41) УБИ.121. Угроза повреждения системного реестра;

42) УБИ.122. Угроза повышения привилегий;

43) УБИ.124. Угроза подделки записей журнала регистрации событий;

44) УБИ.127. Угроза подмены действия пользователя путем обмана;

45) УБИ.128. Угроза подмены доверенного пользователя;

46) УБИ.132. Угроза получения предварительной информации об объекте;

47) УБИ.139. Угроза преодоления физической защиты;

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

49) УБИ.145. Угроза пропуска проверки целостности программного обеспечения;

50) УБИ.152. Угроза удаления аутентификационной информации;

51) УБИ.155. Угроза утраты вычислительных ресурсов;

52) УБИ.156. Угроза утраты носителей информации;

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

54) УБИ.158. Угроза форматирования носителей информации;

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

56) УБИ.167. Угроза заражения компьютера при посещении неблагонадёжных сайтов;

57) УБИ.168. Угроза «кражи» учётной записи доступа к сетевым сервисам;

58) УБИ.170. Угроза неправомерного шифрования информации;

59) УБИ.171. Угроза скрытного включения вычислительного устройства в состав бот-сети;

60) УБИ.172. Угроза распространения «почтовых червей»;

61) УБИ.174. Угроза «фарминга»;

62) УБИ.175. Угроза «фишинга»;

63) УБИ.176. Угроза нарушения технологического (производственного) процесса из-за временных задержек, вносимых средством защиты;

64) УБИ.178. Угроза несанкционированного использования системных и сетевых утилит;

65) УБИ.179. Угроза несанкционированной модификации защищаемой информации;

66) УБИ.182. Угроза физического устаревания аппаратных компонентов;

67) УБИ.185. Угроза несанкционированного изменения параметров настройки средств защиты информации;

68) УБИ.186. Угроза внедрения вредоносного кода через рекламу, сервисы и контент;

69) УБИ.187. Угроза несанкционированного воздействия на средство защиты информации;

70) УБИ.188. Угроза подмены программного обеспечения;

71) УБИ.189. Угроза маскирования действий вредоносного кода;

72) УБИ.190. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;

73) УБИ.192. Угроза использования уязвимых версий программного обеспечения;

74) УБИ.193. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;

75) УБИ.195. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы;

76) УБИ.197. Угроза хищения аутентификационной информации из временных файлов cookie;

77) УБИ.198. Угроза скрытной регистрации вредоносной программой учетных записей администраторов;

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

25. Актуальные угрозы безопасности в разноплановых информационных системах, которые могут быть нейтрализованы только с помощью средств криптографической защиты, определяются оператором информационной системы персональных данных в частных моделях угроз.