КОМИТЕТ СТАВРОПОЛЬСКОГО КРАЯ
ПО ДЕЛАМ НАЦИОНАЛЬНОСТЕЙ И КАЗАЧЕСТВА

ПРИКАЗ

20 мая 2019 г. г. Ставрополь № 40/од

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета Ставропольского края по делам национальностей и казачества

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» с учётом содержания персональных данных, обрабатываемых в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета Ставропольского края по делам национальностей и казачества, характера и способов их обработки

ПРИКАЗЫВАЮ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета Ставропольского края по делам национальностей и казачества, согласно приложению к настоящему приказу.

2. Контроль за выполнением настоящего приказа оставляю за собой.

3. Настоящий приказ вступает в силу со дня его подписания.

Председатель комитета А.В.Писаренко

КОМИТЕТ СТАВРОПОЛЬСКОГО КРАЯ ПО ДЕЛАМ НАЦИОНАЛЬНОСТЕЙ И КАЗАЧЕСТВА

Приложение

к приказу комитета
Ставропольского края по делам
национальностей и казачества
от 20.05.2019 г. № 40/од

УГРОЗЫ

безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых для осуществления деятельности комитета Ставропольского края по делам национальностей и казачества

I. Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых для осуществления деятельности комитета Ставропольского края по делам национальностей и казачества (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 Банке данных угроз безопасности информации рекомендованным информационным сообщением Федеральной службы по техническому и экспортному контролю № 240/22/879 от 06 марта 2015 г. (далее – Банк данных угроз), 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. Уточнение и дополнение актуальных угроз безопасности осуществляется приказом комитета (далее – проект приказа о внесении изменений).

Комитетом подготавливается проект приказ о внесении изменений и направляется на согласование в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности и федеральный орган исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (далее – уполномоченные органы) в течении 30 дней со дня включения сведений в Банк данных угроз об угрозах безопасности информации с учётом структурно-функциональных характеристик информационной системы комитета.

Приказ комитета о внесении изменений издается комитетом в течение 10 рабочих дней со дня получения положительных замечаний от уполномоченных органов.

5. В комитете Ставропольского края по делам национальностей и казачества 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 или в бумажном виде.

7. Перечень персональных данных, обрабатываемых с использованием информационных систем, определяется комитета Ставропольского края по делам национальностей и казачества от 25 ноября 2014 г. № 84/од «Об утверждении Перечня персональных данных, обрабатываемых в комитете Ставропольского края по делам национальностей и казачества в связи с реализацией трудовых отношений».

8. В комитете Ставропольского края по делам национальностей и казачества создается и эксплуатируется информационная система, которая может 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 комитета Ставропольского края по делам национальностей и казачества, 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 комитета Ставропольского края по делам национальностей и казачества.

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

Помещения, в которых размещаются однотипные информационные системы, оборудованы средствами контроля доступа, а также осуществляется их физическая охрана.

Здание комитета Ставропольского края по делам национальностей и казачества оборудовано системами видео наблюдения.

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 комитета Ставропольского края по делам национальностей и казачества.

12. Оператором информационных систем управления персоналом и информационной системы управления финансами выступает комитета Ставропольского края по делам национальностей и казачества.

13. Информационные системы управления персоналом и информационная система управления финансами являются локальными и размещаются в здании комитета Ставропольского края по делам национальностей и казачества.

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.

III. Актуальные угрозы безопасности

15. Актуальными угрозами безопасности в однотипных информационных системах являются:

1) УБИ.006 Угроза внедрения кода или данных;

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

3) УБИ.008 Угроза восстановления аутентификационной информации;

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

5) УБИ.017 Угроза доступа/перехвата/изменения HTTP cookies;

6) УБИ.019 Угроза заражения DNS-кеша;

7) УБИ.023 Угроза изменения компонентов системы;

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

9) УБИ.030 Угроза использования информации идентификации/ аутентификации, заданной по умолчанию;

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

11) УБИ.034 Угроза использования слабостей протоколов сетевого/локального обмена данными;

12) УБИ.049 Угроза нарушения целостности данных кеша;

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

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

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

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

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

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

19) УБИ.086 Угроза несанкционированного изменения аутентификационной информации;

20) УБИ.088 Угроза несанкционированного копирования защищаемой информации;

21) УБИ.089 Угроза несанкционированного редактирования реестра;

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

23) УБИ.091 Угроза несанкционированного удаления защищаемой информации;

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

25) УБИ.099 Угроза обнаружения хостов;

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

27) УБИ.103 Угроза определения типов объектов защиты;

28) УБИ.104 Угроза определения топологии вычислительной сети;

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

30) УБИ.121 Угроза повреждения системного реестра;

31) УБИ.122 Угроза повышения привилегий;

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

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

34) УБИ.128 Угроза подмены доверенного пользователя;

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

36) УБИ.139 Угроза преодоления физической защиты;

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

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

39) УБИ.152 Угроза удаления аутентификационной информации;

40) УБИ.153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

41) УБИ.155 Угроза утраты вычислительных ресурсов;

42) УБИ.156 Угроза утраты носителей информации;

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

44) УБИ.158 Угроза форматирования носителей информации;

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

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

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

48) УБИ.170 Угроза неправомерного шифрования информации;

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

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

51) УБИ.174 Угроза «фарминга»;

52) УБИ.175 Угроза «фишинга»;

53) УБИ.176 Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты;

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

55) УБИ.179 Угроза несанкционированной модификации защищаемой информации;

56) УБИ.182 Угроза физического устаревания аппаратных компонентов;

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

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

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

60) УБИ.188 Угроза подмены программного обеспечения;

61) УБИ.189 Угроза маскирования действий вредоносного кода;

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

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

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

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

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

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

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

16. 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.