ПРАВИТЕЛЬСТВО КРАСНОЯРСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

06.09.2016 г. Красноярск № 445-п

Об утверждении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Красноярского края

В соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», статьей 103 Устава Красноярского края, учитывая приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденную заместителем директора ФСТЭК России 15.02.2008, ПОСТАНОВЛЯЮ:

1. Утвердить угрозы безопасности персональных данных, актуальные при их обработке в информационных системах персональных данных органов исполнительной власти Красноярского края согласно приложению.

2. Опубликовать постановление на «Официальном интернет-портале правовой информации Красноярского края» (www.zakon.krskstate.ru).

3. Постановление вступает в силу в день, следующий за днем его официального опубликования.

Первый заместитель
Губернатора края –
председатель
Правительства края В.П. Томенко

Приложение
к постановлению Правительства
Красноярского края
от 06.09.2016 № 445-п

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Красноярского края

1. Угрозы несанкционированного доступа на рабочих местах, связанные с действиями нарушителей, имеющих доступ к информационным системам персональных данных, включая пользователей информационных систем персональных данных, реализующие угрозы непосредственно в информационных системах персональных данных.

2. Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой.

3. Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения несанкционированного доступа программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах).

4. Угрозы внедрения вредоносных программ.

5. Угрозы выявления паролей.

6. Угрозы типа «Отказ в обслуживании».

7. Угрозы удаленного запуска приложений.

8. Угрозы внедрения по сети вредоносных программ.

9. Угрозы «Анализа сетевого трафика» с перехватом передаваемой из информационных систем персональных данных и принимаемой в информационные системы персональных данных из внешних сетей информации.

10. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций информационных систем персональных данных, топологии сети, открытых портов и служб, открытых соединений.

11. Угрозы внедрения ложного объекта, как в информационные системы персональных данных, так и во внешних сетях.

12. Угрозы подмены доверенного объекта.

13. Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных, как внутри сети, так и во внешних сетях.

14. Угрозы среды виртуализации.

15. Угрозы утечки акустической (речевой) информации.

16. Угрозы утечки видовой информации.

17. Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок.

18. Угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств, с целью нарушения безопасности защищаемых средствами криптографической защиты информации (далее – СКЗИ) персональных данных или создания условий для этого (далее – атака) при нахождении в пределах контролируемой зоны.

19. Угрозы проведения атаки на этапе эксплуатации СКЗИ на следующие объекты:

1) документацию на СКЗИ и компоненты среды функционирования (далее – СФ) СКЗИ;

2) 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.

20. Угрозы получения, в рамках предоставленных полномочий, а также в результате наблюдений, следующей информации:

1) сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

2) сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

3) сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.

21. Угрозы использования штатных средств информационных систем персональных данных, ограниченного мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

22. Угрозы физического доступа к СВТ, на которых реализованы СКЗИ и СФ.

23. Угрозы возможностей воздействия на аппаратные компоненты СКЗИ и СФ, ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

24. Угрозы создания способов, подготовки и проведения атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (не декларированных) возможностей прикладного программного обеспечения.

25. Угрозы проведения лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченного мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

26. Угрозы проведения 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 программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ.

27. Угрозы создания способов, подготовки и проведения атак с привлечением специалистов в области использования для реализации атак недокументированных (не декларированных) возможностей системного программного обеспечения.

28. Угрозы возможностей располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.

29. Угрозы возможностей воздействовать на любые компоненты СКЗИ и СФ.