ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 8 ноября 2016 года № 357
г. Курган

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в Правительстве Курганской области и подведомственных Правительству Курганской области государственных учреждениях

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Правительство Курганской области ПОСТАНОВЛЯЕТ:

1. Утвердить перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в Правительстве Курганской области и подведомственных Правительству Курганской области государственных учреждениях (далее — Перечень) согласно приложению к настоящему постановлению.

2. Управлению информационных технологий Правительства Курганской области и подведомственным Правительству Курганской области государственным учреждениям при разработке частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных адаптировать Перечень.

3. Контроль за исполнением настоящего постановления возложить на заместителя Губернатора Курганской области - руководителя Аппарата Правительства Курганской области.

Губернатор
Курганской области А.Г. Кокорин

Усанин С.Н.
(3522) 42-92-03

Приложение к постановлению
Правительства Курганской области
от «8» ноября 2016 года №357
«Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в Правительстве Курганской области и подведомственных Правительству Курганской области государственных учреждениях»

Перечень
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в Правительстве Курганской области и подведомственных Правительству Курганской области государственных учреждениях

Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю Российской Федерации

1. Угроза внедрения кода или данных.
2. Угроза воздействия на программы с высокими привилегиями.
3. Угроза восстановления аутентификационной информации.
4. Угроза выхода процесса за пределы виртуальной машины.
5. Угроза доступа к защищаемым файлам с использованием обходного пути.
6. Угроза доступа/перехвата/изменения HTTP cookies.
7. Угроза избыточного выделения оперативной памяти.
8. Угроза изменения системных и глобальных переменных.
9. Угроза искажения XML-схемы.
10. Угроза искажения вводимой и выводимой на периферийные устройства информации.
11. Угроза использования механизмов авторизации для повышения привилегий.
12. Угроза использования слабостей протоколов сетевого/локального обмена данными.

13. Угроза нарушения изоляции пользовательских данных внутри виртуальной машины.
14. Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия.
15. Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин.
16. Угроза нарушения целостности данных кеша.
17. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов.
18. Угроза некорректного задания структуры данных транзакции.
19. Угроза неправомерных действий в каналах связи.
20. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.
21. Угроза несанкционированного доступа к аутентификационной информации.
22. Угроза несанкционированного доступа к виртуальным каналам передачи.
23. Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети.
24. Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение.
25. Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети.
26. Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин.
27. Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети.
28. Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации.
29. Угроза несанкционированного управления буфером.
30. Угроза несанкционированного управления синхронизацией и состоянием.
31. Угроза несанкционированного управления указателями.
32. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
33. Угроза обнаружения хостов.
34. Угроза обхода некорректно настроенных механизмов аутентификации.
35. Угроза опосредованного управления группой программ через совместно используемые данные.
36. Угроза определения типов объектов защиты.
37. Угроза определения топологии вычислительной сети.

38. Угроза ошибки обновления гипервизора.
39. Угроза перехвата данных, передаваемых по вычислительной сети.
40. Угроза повреждения системного реестра.
41. Угроза подмены действия пользователя путем обмана.
42. Угроза подмены доверенного пользователя.
43. Угроза подмены субъекта сетевого доступа.
44. Угроза получения предварительной информации об объекте защиты.
45. Угроза приведения системы в состояние «отказ в обслуживании».
46. Угроза пропуска проверки целостности программного обеспечения.
47. Угроза сбоя обработки специальным образом измененных файлов.
48. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.
49. Угроза утраты вычислительных ресурсов.
50. Угроза заражения компьютера при посещении неблагонадежных сайтов.
51. Угроза неправомерного шифрования информации.
52. Угроза скрытного включения вычислительного устройства в состав бот-сети.
53. Угроза распространения «почтовых червей».
54. Угроза «спама» веб-сервера.
55. Угроза «фарминга».
56. Угроза «фишинга».
57. Угроза несанкционированной модификации защищаемой информации.

Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации

Таблица 1. Обобщенные возможности источников атак

№	Обобщенные возможности источников атак	Да/нет
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы средства криптографической защиты информации (далее - СКЗИ) и среда их функционирования	Да

№	Обобщенные возможности источников атак	Да/нет
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	Нет
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

Таблица 2. Актуальные угрозы безопасности персональных данных

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1.	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	
1.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты среды функционирования СКЗИ (далее - СФ); - помещения, в которых находится совокупность программных и технических	Не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ		постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения
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 СВТ, на которых реализованы СКЗИ и СФ	Не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается ресурсы информационных систем персональных данных (далее - ИСПДн), обеспечивается в соответствии с контрольно-пропускным режимом; сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации
1.4.	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной	Не актуально	Проводятся работы по подбору персонала; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИСПДн используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты
2.1.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода
2.2.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в	Не актуально	Проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
3.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических,

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты
3.2.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности
3.3.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		высокая стоимость и сложность подготовки реализации возможности
4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты
4.2.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3.	Возможность воздействовать на любые компоненты СКЗИ и СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности