ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

ДЕПАРТАМЕНТ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

17 апреля 2018 года № 45-ОД
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 Департаменте экономического развития Курганской области и подведомственном Департаменту экономического развития Курганской области государственном унитарном предприятии

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

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 Департаменте экономического развития Курганской области и подведомственном Департаменту экономического развития Курганской области государственном унитарном предприятии (далее — Перечень) согласно приложению к настоящему приказу.

2. При разработке частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных в Департаменте экономического развития Курганской области и подведомственном Департаменту экономического развития Курганской области государственном унитарном предприятии адаптировать Перечень.

3. Контроль за исполнением настоящего приказа возложить на первого заместителя директора Департамента экономического развития Курганской области.

Заместитель Губернатора Курганской области —
директор Департамента экономического развития
Курганской области С.А. Чебыкин

Приложение к приказу
Департамента экономического развития Курганской области
от 17 апреля 2018 года № 45-ОД
«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 Департаменте экономического развития Курганской области и подведомственном Департаменту экономического развития Курганской области государственном унитарном предприятии»

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 Департаменте экономического развития Курганской области и подведомственном Департаменту экономического развития Курганской области государственном унитарном предприятии

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 доступа к защищаемым файлам с использованием обходного пути.
5. Угроза доступа/перехвата/изменения HTTP cookies.
6. Угроза избыточного выделения оперативной памяти.
7. Угроза изменения системных и глобальных переменных.
8. Угроза искажения XML-схемы.
9. Угроза искажения вводимой и выводимой на периферийные устройства информации.
10. Угроза использования механизмов авторизации для повышения привилегий.
11. Угроза использования слабостей протоколов сетевого/локального обмена данными.
12. Угроза нарушения целостности данных кеша.
13. Угроза некорректного задания структуры данных транзакции.
14. Угроза неправомерных действий в каналах связи.
15. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети,

16. Угроза несанкционированного доступа к аутентификационной информации.
17. Угроза несанкционированного доступа к виртуальным каналам передачи.
18. Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети.
19. Угроза несанкционированного управления буфером.
20. Угроза несанкционированного управления синхронизацией и состоянием.
21. Угроза несанкционированного управления указателями.
22. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
23. Угроза обнаружения хостов.
24. Угроза обхода некорректно настроенных механизмов аутентификации.
25. Угроза опосредованного управления группой программ через совместно используемые данные.
26. Угроза определения типов объектов защиты.
27. Угроза определения топологии вычислительной сети.
28. Угроза передачи данных по скрытым каналам.
29. Угроза перехвата данных, передаваемых по вычислительной сети.
30. Угроза повреждения системного реестра.
31. Угроза подмены действия пользователя путем обмана.
32. Угроза подмены доверенного пользователя.
33. Угроза подмены субъекта сетевого доступа.
34. Угроза получения предварительной информации об объекте защиты.
35. Угроза приведения системы в состояние "отказ в обслуживании".
36. Угроза пропуска проверки целостности программного обеспечения.
37. Угроза сбоя обработки специальным образом измененных файлов.
38. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.
39. Угроза утраты вычислительных ресурсов.
40. Угроза заражения компьютера при посещении неблагонадежных сайтов.
41. Угроза неправомерного шифрования информации.
42. Угроза скрытного включения вычислительного устройства в состав бот-сети.
43. Угроза распространения "почтовых червей".
44. Угроза "спама" веб-сервера.
45. Угроза "фарминга".
46. Угроза "фишинга".
47. Угроза несанкционированной модификации защищаемой информации.
48. Угроза внедрения вредоносного кода через рекламу, сервисы и контент.
49. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет.
50. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика.
51. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы.
52. Угроза хищения аутентификационной информации из временных файлов cookie.
53. Угроза скрытной регистрации вредоносной программой учетных записей администраторов.
54. Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты.

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 СКЗИ и среда их функционирования	Да
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 (далее — СФ); - помещения, в которых находится совокупность программных и технических элементов систем обработки данных,	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. Помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения

	способных функционировать самостоятельно или в составе других систем (далее — СВТ), на которых реализованы СКЗИ и СФ		постоянного закрытия дверей помещений на замок и их открытия 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 располагаются ресурсы 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 системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	Проводятся работы по подбору персонала. 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. 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 доступ, 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 информационной системе, в которой используется СКЗИ, и	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.

	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, 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, 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 в области разработки и анализа СКЗИ и СФ, в том числе	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.

	с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		
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 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, 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.