ПОСТАНОВЛЕНИЕ

ПРАВИТЕЛЬСТВА ЛИПЕЦКОЙ ОБЛАСТИ

06 сентября 2024 года г. Липецк № 520

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Правительства Липецкой области

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных", по согласованию с Федеральной службой по техническому и экспертному контролю от 17 ноября 2023 года № 22/5563 и Федеральной службой безопасности Российской Федерации от 17 июня 2024 года № 8983-Мл Правительство Липецкой области постановляет:

Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Правительства Липецкой области (приложение).

Губернатор
Липецкой области И.Г. Артамонов

Правительство Липецкой области * Управление делами * Отдел делопроизводства и документационного обеспечения

Приложение
к постановлению Правительства
Липецкой области
«Об определении угроз безопасности
персональных данных, актуальных
при обработке персональных данных
в информационных системах
персональных данных
Правительства Липецкой области»

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Правительства Липецкой области

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных Правительства Липецкой области (далее – ИСПДн), являются:

1) угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее - СКЗИ);

2) угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности персональных данных, защищаемых с использованием СКЗИ, или создания условий для этого.

2. Угрозы безопасности персональных данных, защищаемых без использования СКЗИ, включают:

1) угрозы воздействия вредоносного кода и (или) вредоносных программ (вирусов), внешних по отношению к ИСПДн;

2) угрозы несанкционированного доступа к информации через сети международного обмена;

3) угрозы разглашения информации, ее модификации или уничтожения сотрудниками, допущенными к ее обработке;

4) угрозы использования методов социального инжиниринга к лицам, обладающим полномочиями в ИСПДн;

5) угрозы несанкционированного доступа к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей ИСПДн;

6) угрозы утраты (потери) носителей персональных данных и аппаратных средств, включая переносные персональные компьютеры пользователей ИСПДн;

7) угрозы несанкционированного доступа к персональным данным лицами, обладающими полномочиями в ИСПДн, в том числе в ходе создания,

эксплуатации, технического обслуживания и (или) ремонта, модернизации, вывода из эксплуатации ИСПДн;

8) угрозы несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в ИСПДн, с использованием уязвимостей в организации защиты персональных данных;

9) угрозы несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в ИСПДн, с использованием уязвимостей в программном обеспечении ИСПДн;

10) угрозы несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в ИСПДн, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных, в том числе с использованием протоколов межсетевого взаимодействия;

11) угрозы несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в ИСПДн, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации;

12) угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений;

13) угрозы, связанные с возможностями использования информационных технологий (технологии виртуализации, беспроводные технологии, облачные технологии, технологии удаленного доступа и иные технологии);

14) угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации.

3. Угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности персональных данных, защищаемых с использованием СКЗИ, или создания условий для этого определяются актуальностью использования возможностей источников атак[1].

---

[1] Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке 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, утвержденные приказом ФСБ России от 10 июля 2014 года № 378.

Оценка возможностей источников атак

Таблица 1

№ п/п	Обобщенные возможности источников атак	Да/ нет
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны (далее – КЗ)	да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования (далее – СФ)	нет
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ с физическим доступом к АС, на которых реализованы СКЗИ и СФ	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 СФ СКЗИ)	нет

Актуальность использования возможностей источников атак

Таблица 2

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.	Проведение атаки при нахождении в пределах КЗ	не актуально	Проводятся работы по подбору персонала. Доступ в КЗ, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом. Помещения, в которых располагаются СКЗИ, оснащены дверями с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода. Утверждены порядок доступа в помещения и список лиц, имеющих право доступа в помещения, в которых располагаются СКЗИ. Пользователи СКЗИ ознакомлены с правилами работы с СКЗИ и ответственностью за несоблюдение правил обеспечения безопасности информации. Сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и 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; сертифицированные средства антивирусной защиты. Работа представителей технических и вспомогательных служб в помещениях, где располагаются СКЗИ, проводится в присутствии сотрудников по эксплуатации СКЗИ.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			На системах вычислительной техники (далее – СВТ), в которых установлены СКЗИ, используются сертифицированные средства защиты информации от несанкционированного доступа.
2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты СФ, помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других СВТ, на которых реализованы СКЗИ и СФ	не актуально	Проводятся работы по подбору персонала. Доступ в КЗ, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом. Документация на СКЗИ хранится у ответственного за СКЗИ в металлическом шкафу. Помещения, в которых располагаются СКЗИ, оснащены дверями с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода. Утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ.
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 КЗ 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 КЗ 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.
4.	Использование штатных средств ИСПДн,	не актуально	Проводятся работы по подбору персонала.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ограниченное мерами, реализованными в информационной системе, в которой используется ИСПДн, и направленными на предотвращение и пресечение несанкционированных действий		Помещения, в которых располагаются СВТ, на которых реализованы СКЗИ и СФ, оснащены входными дверями 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 доступа; сертифицированные средства антивирусной защиты.
5.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	не актуально	Проводятся работы по подбору персонала. Помещения, в которых располагаются СВТ, на которых реализованы СКЗИ и СФ, оснащены входными дверями 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. Доступ в КЗ и помещения, где располагаются СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом.
6.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ,	не актуально	Проводятся работы по подбору персонала. Доступ в КЗ и помещения, где располагаются СВТ, на которых

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		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, где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации.
7.	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 программного обеспечения (далее – ПО)	не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Проводятся работы по подбору персонала. Доступ в КЗ 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, где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			эксплуатации. Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам. Осуществляется регистрация и учет действий пользователей. На автоматизированных рабочих местах (далее – АРМ) и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
8.	Проведение лабораторных исследований СКЗИ, используемых вне КЗ, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности.
9.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в т.ч. с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности.
10.	Создание способов, подготовка и проведение атак с привлечением	не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО		Высокая стоимость и сложность подготовки реализации возможности. Проводятся работы по подбору персонала. Доступ в КЗ 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, 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.
11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	не актуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности.
12.	Возможность	не актуально	Не осуществляется обработка

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	воздействовать на любые компоненты СКЗИ и СФ		сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности.