Администрация Главы РСО-Алания и Правительства РСО-Алания
ЗАРЕГИСТРИРОВАНО
2 12 2024 г.
№ 0344-24-2

КОМИТЕТ
РЕСПУБЛИКИ СЕВЕРНАЯ ОСЕТИЯ-АЛАНИЯ
ПО ЗАНЯТОСТИ НАСЕЛЕНИЯ

ПРИКАЗ

«23» 11 2024 г. № 65-ф

г. Владикавказ

Об определении угроз безопасности персональных данных ПДн в ИСПДн Комитета РСО-Алания по занятости населения

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», Федеральным законом от 12 декабря 2023 года №565-ФЗ «О занятости населения в Российской Федерации» **приказываю**:

1. Определить угрозы безопасности персональных данных ПДн в информационных системах персональных данных ИСПДн Комитета РСО-Алания по занятости населения, определенных законодательством Российской Федерации, согласно приложению к настоящему приказу.
2. Козаевой И.Б. - ведущему советнику отдела организационной, кадровой работы и противодействия коррупции ознакомить с приказом касающихся лиц под роспись.
3. Контроль исполнения приказа возложить на начальника отдела информационных технологий и автоматизации Чельдиеву М.К.

Заместитель председателя **Э.Л. Авакова**

Приложение
к приказу Комитета РСО-Алания
по занятости населения
от 12.11 2024 года № 65-ф

Угрозы
безопасности персональных данных, актуальные при обработке персональных данных Комитета Республики Северная Осетия-Алания по занятости населения, определенных законодательством Российской Федерации

В соответствии с законодательством Российской Федерации определен перечень угроз безопасности персональных данных (далее- ПДн), актуальный при обработке ПДн в информационных системах персональных данных (далее- ИСПДн) Комитета Республики Северная Осетия -Алания по занятости населения (далее-Комитет).

Угрозами безопасности ПДн эксплуатируемых в ИСПДн Комитета являются:

-угрозы безопасности ПДн, защищаемых без использования средств криптографической защиты информации (далее – СКЗИ);

-угрозы реализации целенаправленных действий с использованием аппаратных или программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ ПДн или созданий условий для этого.

1.Для персональных данных, защищаемых без СКЗИ, актуальными являются угрозы:

1.1 Определяемые функционированием технических, программно-технических и программных средств, обеспечивающим хранение, обработку и передачу информации.

1.2 Несанкционированного доступа к ПДн лицам, обладающими пользовательскими правами доступа к информационным системам, правами доступа к администрированию программных, программно-аппаратных средств, средств защиты информации, входящих в состав информационных систем, в ходе создания, эксплуатации, технического обслуживания и ремонта, модернизации, выхода из эксплуатации информационных систем.

1.3 Применение вредоносного кода, вредоносной программы в зоне эксплуатации ИСПДн.

1.4 Социального и психологического воздействия на лиц, обладающих правами доступа к информационным системам, правами доступа к администрированию программных, программно-аппаратных средств, средств защиты информации, входящих в состав информационных систем.

1.5 Несанкционированного доступа к отчуждаемым носителям ПДн, включая переносные технические средства пользователей информационных систем.

1.6 Воздействие на отчуждаемые носители ПДн, включая переносные технические средства пользователей информационных систем.

2. Несанкционированный доступ к ПДн лицам, не обладающим правами доступа к информационным системам, правами доступа к администрированию программных, программно-аппаратных средств, средств защиты информации, входящих в состав информационных систем, с использованием уязвимостей являются угрозы:

2.1 В организации защиты ПДн.

2.2 В обеспечении защиты сетевого взаимодействия и каналов передачи данных, в том числе с использованием протоколов межсетевого взаимодействия.

2.3 В обеспечении защиты вычислительных и информационных сетей, вызванных несоблюдением требований по эксплуатации средств защиты информации.

2.4 В системном и прикладном программном обеспечении информационных сетей.

2.5 Использование современных информационных технологий, связанных с возможностью использования новых информационных технологий (технологии виртуализации, беспроводные технологии, облачные технологии, технологии удаленного доступа и иные современные технологии).

3. Угрозы целенаправленных действий с использованием аппаратных или программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого включают:

3.1 Создание способов, подготовку и проведение атак без привлечения специалистов в области анализа СКЗИ.

3.2 Создание способов, подготовку и проведение атак на различных этапах жизненного цикла СКЗИ.

3.3 Проведение атак нарушителями, находящимися вне пространства, в пределах которого осуществляется контроль за техническими средствами зоны наблюдения.

3.4 Угрозы проведения атак нарушителями, находящимися вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц или технических средств.

3.5 Угрозы проведения на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ, атаки путем внесения несанкционированных изменений в СКЗИ, документацию на СКЗИ или в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и которые в совокупности представляют среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ.

4. Угрозы проведения атак на этапе эксплуатации СКЗИ распространяются на:

4.1 Персональные данные.

4.2 Ключевую, аутентифицирующую и парольную информацию СКЗИ.

4.3 Программные компоненты СКЗИ.

4.4 Аппаратные компоненты СКЗИ.

4.5 Программные компоненты среды функционирования СКЗИ, включая базовую систему ввода (вывода).

4.6 Аппаратные компоненты среды функционирования СКЗИ.

4.7 Данные, передаваемые по каналам связи.

5. Угрозы доступные из источников, находящихся в свободном доступе (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационных системах, в которых используются СКЗИ:

5.1 Общие сведения об информационных системах, в которых используются СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационных систем).

5.2 Сведения об информационных технологиях, базах данных, аппаратных средствах, программном обеспечении, используемых в информационных системах совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторских документах на информационные технологии, базы данных, аппаратные средства, программное обеспечение, используемые в информационных системах совместно с СКЗИ.

5.3 Содержания конструкторской документации на СКЗИ.

5.4 Содержания документации на аппаратные и программные компоненты СКЗИ и среду функционирования СКЗИ.

5.5 Общие сведения о защищаемой информации ПДн, используемые в процессе эксплуатации СКЗИ.

5.6 Сведения о каналах связи, по которым передаются персональные данные, защищаемые с использованием СКЗИ.

5.7 Сведения, получаемые в результате анализа сигналов от аппаратных компонентов СКЗИ и среды функционирования СКЗИ.

6. Угрозы, применяемые в специально разработанных аппаратных средствах и программном обеспечении.

7. Угрозы, допустимые на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту), атаки действий, осуществляемых при подготовке или проведении атаки каналов распространения сигналов, сопровождающих функционирование СКЗИ и среды функционирования СКЗИ.

8. Угрозы, актуальные во время проведения атак при нахождении в пределах контролируемой зоны ИСПДн.

9. Угрозы проведения атак, допустимые на этапе эксплуатации СКЗИ:

9.1 На документацию СКЗИ и компоненты среды функционирования СКЗИ.

9.2 Помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и среда функционирования СКЗИ.

10. Угрозы допустимые в рамках предоставленных полномочий, а также в результате наблюдений:

10.1 Сведений о физических мерах защиты объектов, в которых размещены ресурсы информационных систем.

10.2 Сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационных систем.

10.3 Сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы СКЗИ и среда функционирования СКЗИ.

11. Угрозы несанкционированного физического доступа к средствам вычислительной техники, на которых реализованы СКЗИ и среда функционирования СКЗИ.

12. Угрозы, связанные с наличием у нарушителя аппаратных компонентов СКЗИ и среды функционирования СКЗИ, реализованных в информационных системах, в которых используются СКЗИ.

13. Угрозы с возможностью получения данных из открытых источников.

13.1 Угрозы, связанные с получением данных, передаваемых в открытом виде по каналам связи, не защищенном от несанкционированного доступа к информации организационными и техническими мерами, возможны через:

-открытые данные, содержащие сведения о нарушениях правил эксплуатации СКЗИ в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

-сведения о неисправностях и сбоях аппаратных компонентов СКЗИ, обнаруженных в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

-сведения, находящиеся в свободном доступе или используемых за пределами контролируемой зоны автоматизированных систем программного обеспечения, включая аппаратные и программные компоненты СКЗИ;

-проведение на этапе эксплуатации атак из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

-проведение атак при нахождении в пределах контролируемой зоны ИСПДн.

14. Угрозы, связанные с возможностью уничтожения на этапе эксплуатации СКЗИ и несанкционированным доступом к следующим объектам.

14.1 Документации на СКЗИ и компонентам ИСПДн.

14.2 Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ.

15. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

15.1 Сведения о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

15.2 Сведения о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

15.3 Сведения о мерах по разграничению доступа в помещения, в которых находятся ИСПДн, на которых реализованы СКЗИ;

15.4 Получение несанкционированного физического доступа к ИСПДн, на которых реализованы СКЗИ;

15.5 Наличие у нарушителя аппаратных компонентов СКЗИ, реализованных в информационной системе, в которой используется СКЗИ.