

КУРГАНСКАЯ ОБЛАСТЬ

ЛЕБЯЖЬЕВСКИЙ МУНИЦИПАЛЬНЫЙ ОКРУГ КУРГАНСКОЙ ОБЛАСТИ

ГЛАВА ЛЕБЯЖЬЕВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

КУРГАНСКОЙ ОБЛАСТИ

**П О С Т А Н О В Л Е Н И Е**

От 22 мая 2023 года № 12

р. п. Лебяжье

1. **Об обращении со средствами криптографической защиты информации**
2. **защищенной сети передачи данных**

В целях исполнения требований Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», а также иных нормативных правовых актов Российской Федерации по безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации (далее СКЗИ) защищенной сети передачи данных

ПОСТАНОВЛЯЮ:

1. Назначить ответственным лицом за организацию работ по криптографической защите информации, в том числе за техническое обслуживание и эксплуатацию СКЗИ защищенной сети передачи данных Администрации Лебяжьевского муниципального округа Герцена А.С.

2. Ответственному лицу в своей работе руководствоваться внутренними организационно-распорядительными документами по защите информации, положениями законодательства Российской Федерации по защите информации с использованием СКЗИ, в частности:

- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной Приказом ФАПСИ от 13 июня 2001 года № 152;

- Составом и содержанием 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, утвержденным ФСБ России от 10 июля 2014 года № 378.

3. Утвердить перечень спецпомещений, а также установить границы контролируемой зоны по внешнему периметру стен (включая окна и двери) спецпомещений, в которых располагаются СКЗИ, эксплуатационные и технические документы к ним, ключевые документы согласно приложению 1 к настоящему постановлению.

4. Утвердить инструкцию о порядке доступа в спецпомещения согласно приложению 2 к настоящему постановлению.

5. Утвердить перечень мест хранения эксплуатационных и технических документов на СКЗИ, ключевых документов. согласно приложению 3 к настоящему постановлению.

6. Утвердить модель нарушителя согласно приложению 4 к настоящему постановлению.

7. Утвердить перечень лиц, допущенных в помещения, где установлены СКЗИ или хранятся ключевые документы к ним, согласно приложению 5 к настоящему постановлению.

8. Контроль за исполнением настоящего постановления оставляю за собой.

1. Глава Лебяжьевского муниципального округа
2. Курганской области А.Р.БАРЧ
3. Исп Герцен А.С.
4. Тел. 9-00-21
5. Приложение 1 к постановлению
6. Главы Лебяжьевского
7. муниципального округа
8. Курганской области
9. от 22 мая 2023 года № 12
10. «Об обращении со средствами
11. криптографической защиты информации
12. защищенной сети передачи данных»

Перечень спецпомещений

Спецпомещения – помещения, где установлены средства криптографической защиты информации или хранятся ключевые документы к ним

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование объекта информатизации** | **Адрес (место) расположения** | **Этаж и номер (обозначение) спецпомещения** |
| 1. . | Администрация Лебяжьевского Муниципального округа Курганской области | 641500, Курганская обл., Лебяжьевский район, р.п. Лебяжье, ул. Пушкина, дом 14 | , кабинет № 10 |

1. Приложение 2 к постановлению
2. Главы Лебяжьевского
3. муниципального округа
4. Курганской области
5. от 22 мая 2023 года № 12\_
6. «Об обращении со средствами
7. криптографической защиты информации
8. защищенной сети передачи данных»

Инструкция о порядке доступа в спецпомещения

1. Общие положения

1.1. Настоящая инструкция разработана на основе документов:

* «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной Приказом ФАПСИ от 13 июня 2001 г. № 152;
* «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», утвержденный Приказом ФСБ России от 10 июля 2014 г. № 378.

1.2. Настоящая инструкция регламентируют организацию и порядок доступа в спецпомещения[[1]](#footnote-1) Администрации Лебяжьевского Муниципального округа Курганской области (далее – Учреждение).

1.3. Настоящая инструкция разработана в целях обеспечения безопасности конфиденциальной информации, средств вычислительной техники информационных систем, материальных носителей, а также средств криптографической защиты информации.

2. Порядок доступа в помещения

2.1. Доступ в работников оформляется после ознакомления с организационно-распорядительными и техническими документами по защите информации Учреждения.

2.2. Доступ посторонних лиц в помещения осуществляется только ввиду служебной необходимости. При этом, на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с конфиденциальной информацией.

2.3. В нерабочее время помещения должны ставится под охрану. При этом, все окна (при наличии) и двери должны быть надёжно закрыты, документы, содержащие конфиденциальную информацию, убраны в запираемые шкафы (сейфы), средства вычислительной техники выключены, либо заблокированы.

2.4. Вскрытие и запирание (постановка и снятие с охраны) помещений производится работниками Учреждения, имеющими соответствующие права, с отметкой в журнале вскрытия (запирания) помещений.

2.5. Помещения, в которых ведется обработка конфиденциальной информации и расположены средства криптографической информации, должны быть оснащены входными дверьми с замками. Кроме того, должно быть обеспечено постоянное запирание дверей таких помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

2.6. Помещения должны быть оснащены охранной сигнализацией. Результаты периодической проверки исправности сигнализации должны отражаться в журнале.

2.7. При утрате ключа от хранилища или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

3. Внутренний контроль

3.1. Запрещается оставлять спецпомещения без присмотра работников, имеющих допуск в помещения.

3.2. Запрещается оставлять без присмотра находящихся в помещении посторонних лиц, а также, работников, не имеющих допуск в помещения.

3.2. Внутренний контроль за соблюдением порядка доступа в помещения осуществляется ответственным лицом за организацию границ контролируемой зоны Учреждения

1. Приложение 3 к постановлению
2. Главы Лебяжьевского
3. муниципального округа
4. Курганской области
5. от 22 мая 2023 года № 12
6. «Об обращении со средствами
7. криптографической защиты информации
8. защищенной сети передачи данных»

Перечень мест хранения эксплуатационных и технических документов на СКЗИ, ключевых документов

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование объекта информатизации | Адрес (место) расположения | Место хранения (этаж, номер (обозначение) спецпомещения, сведения о хранилище) |
|  | Администрация Лебяжьевского Муниципального округа Курганской области | 641500, Курганская обл., Лебяжьевский район, р.п. Лебяжье, ул. Пушкина, дом 14 | этаж 2, кабинет № 10  сейф, б/н |

1. Приложение 4 к постановлению
2. Главы Лебяжьевского
3. муниципального округа
4. Курганской области
5. от 22 мая 2023 года № 12\_
6. «Об обращении со средствами
7. криптографической защиты информации
8. защищенной сети передачи данных»

|  |
| --- |
| Модель нарушителя |

# Общие положения

* 1. Модель нарушителя разработана в соответствии с Методическими рекомендациями по разработке по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432, а также Составом и содержанием 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, утвержденным Приказом ФСБ России от 10 июля 2014 г. № 378.
  2. Модель нарушителя определяет потенциальных нарушителей и их возможности по реализации угроз безопасности информации в отношении информационных систем с использованием средств криптографической защиты информации (далее – СКЗИ), используемых на объектах информатизации Администрации Лебяжьевского Муниципального округа Курганской области (далее – Учреждение).

# Источники угроз безопасности информации

Виды возможных нарушителей безопасности информации и их цели приведены в таблице 1.

Таблица 1 – Виды потенциальных нарушителей безопасности информации

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Вид нарушителя | Категория нарушителя | Возможные цели реализации угроз безопасности информации |
|  | Специальные службы иностранных государств | Внешний | Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса |
|  | Террористические, экстремистские группировки | Внешний | Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций |
|  | Преступные группы (криминальные структуры) | Внешний | Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса) |
|  | Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса) |
|  | Конкурирующие организации | Внешний | Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды |
|  | Разработчики программных, программно-аппаратных средств | Внутренний | Внедрение дополнительных функциональных возможностей в программные или программноаппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия |
|  | Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | Внешний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ |
|  | Поставщики вычислительных услуг, услуг связи | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ |
|  | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ |
|  | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия |
|  | Авторизованные пользователи систем и сетей | Внутренний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
|  | Системные администраторы и администраторы безопасности | Внутренний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
|  | Бывшие работники (пользователи) | Внешний | Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия |

Перечень потенциальных нарушителей безопасности информации приведен в таблице 2.

Таблица 2 – Перечень потенциальных нарушителей безопасности информации

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Вид нарушителя | Категория нарушителя | Возможные цели реализации угроз безопасности информации |
|  | Отдельные физические лица (хакеры) | Внешний | Любопытство или желание самореализации (подтверждение статуса) |
|  | Преступные группы (криминальные структуры) | Внешний | Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса) |
|  | Авторизованные пользователи системы | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия |

Иные нарушителя признаются неактуальными с связи с тем, что:

* в информационных системах не обрабатываются сведения, составляющие государственную тайну;
* с применением СКЗИ обрабатывается небольшой объем персональных данных;
* разработчики и привлекаемые поставщики несут ответственность, установленную договорами;
* персоналом информационных систем являются обученные работники, выполняющие возложенные функции на основании должностных обязанностей и несущие персональную ответственность за нарушение условий эксплуатации СКЗИ.

Уровни возможностей потенциальных нарушителей по реализации угроз безопасности, приведены в таблице 3.

Таблица 3 – Уровни возможностей потенциальных нарушителей

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Вид нарушителя | Уровень возможностей нарушителя | Описание возможностей |
|  | Отдельные физические лица (хакеры) | Базовые | Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты.  Обладает базовыми компьютерными знаниями и навыками на уровне пользователя |
|  | Преступные группы (криминальные структуры) | Базовые повышенные | Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и  разработанные другими лицами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз.  Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. |
|  | Авторизованные пользователи системы | Базовые | Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты.  Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним |

Обобщенные возможности источников атак приведены в таблице 4.

Таблица 4 – Обобщенные возможности источников атак

|  |  |  |
| --- | --- | --- |
| № п/п | Обобщенные возможности источников атак | Да/нет |
|  | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны | Да |
|  | 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 |
|  | 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 |
|  | 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 |
|  | Возможность привлекать специалистов, имеющих опыт  разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения) | Нет |
|  | 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 |

Уточненные возможности потенциальных нарушителей по реализации угроз безопасности приведены в таблице 5.

Таблица 5 – Уточненные возможности потенциальных нарушителей

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы) | Актуальность использования (применения) для построения и реализации атак | Обоснование отсутствия |
|  | Проведение атаки при нахождении в пределах контролируемой зоны | актуально | - |
|  | Проведение атак на этапе эксплуатации средств криптографической защиты информации на следующие объекты:  - документацию на СКЗИ и компоненты среды функционирования (далее – СФ) СКЗИ;  - 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 | актуально | - |
|  | Получение в рамках предоставленных полномочий, а также в результате наблюдений, следующей информации:  - сведения о физических мерах защиты объектов, в которых размещены ресурсы информационных систем;  - сведения о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационных систем;  - сведения о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ | актуально | - |
|  | Использование штатных средств информационных систем, ограниченное мерами, реализованными в информационных системах, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | актуально | - |
|  | Физический доступ к СВТ, на которых реализованы СКЗИ и СФ | неактуально | * нахождение внешних и внутренних нарушителей внутри контролируемой зоны возможно только в соответствии с установленными правилами доступа; * помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками. Обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; * доступ к СКЗИ и СФ органичен установленными правилами в Учреждении; * 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; * пропускной режим; * 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; * на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты. |
|  | Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационных системах, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | неактуально |
|  | 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 | неактуально |
|  | Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационных системах, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | неактуально |
|  | Проведение 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 ПО, непосредственно использующего вызовы программных функций СКЗИ | неактуально |
|  | Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО | неактуально |
|  | Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ | неактуально |
|  | Возможность воздействовать на любые компоненты СКЗИ и СФ | неактуально |

# 3. Заключительные положения

Учитывая особенности потенциальных нарушителей по реализации угроз безопасности информации должны применяться СКЗИ не ниже класса КС2.

1. Приложение 5 к постановлению
2. Главы Лебяжьевского
3. муниципального округа
4. Курганской области
5. от 22 мая 2023 года № 12\_
6. «Об обращении со средствами
7. криптографической защиты информации
8. защищенной сети передачи данных»

**Перечень лиц, допущенных в помещения, где установлены СКЗИ или хранятся ключевые документы к ним**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Помещение (этаж, номер (обозначение) спецпомещения)** |
|  | Герцен Алексей Сергеевич | Начальник отдела информационных технологий | этаж 2, кабинет № 1,  кабинет № 10 |

1. Спецпомещения – помещения, где установлены средства криптографической защиты информации или хранятся ключевые документы к ним. [↑](#footnote-ref-1)