КУРГАНСКАЯ ОБЛАСТЬ
ЗВЕРИНОГОЛОВСКИЙ МУНИЦИПАЛЬНЫЙ ОКРУГ
ГЛАВА ЗВЕРИНОГОЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

РАСПОРЯЖЕНИЕ

от «31» мая 2023 года № 47-рг
село Звериноголовское

Об обращении со средствами криптографической защиты информации 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 нормативно-правовых актов Российской Федерации по безопасности персональных данных при их обработке в информационных системах персональных данных с использование средств криптографической защиты информации (далее СКЗИ) защищенной сети передачи данных ОБЯЗЫВАЮ:

1. Назначить ответственным лицом за организацию работ по криптографической защите информации, в том числе за техническое обслуживание и эксплуатацию СКЗИ защищенной сети передачи данных, Начальника отдела информационных технологий Администрации Звериноголовского муниципального округа Курганской области.

2. Ответственному лицу в своей работе руководствоваться внутренними организационно-распорядительными документами по защите информации, положениями законодательства Российской Федерации по защите информации с использование 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 «Об утверждении Инструкции 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»;

- составом 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, утвержденным Приказом ФСБ России от 10 июля 2014 N 378 «Об утверждении Состава и содержания 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».

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 в соответствии с приложением 1 к настоящему распоряжению.

4. Утвердить Инструкцию о порядке доступа в спецпомещения согласно приложению 2 к настоящему распоряжению.

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

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

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

8. Контроль за выполнением настоящего распоряжению оставляю за собой.

Временно исполняющий полномочия
Главы Звериноголовского муниципального
округа Курганской области М.А. Панкратова

Приложение 1 к распоряжению Главы Звериноголовского муниципального округа Курганской области от «31» мая 2023 года №47-рг «Об обращении со средствами криптографической защиты информации 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 Звериноголовского муниципального округа Курганской области	641480, Курганская область, Звериноголовский район , село Звериноголовское, улица Чапаева, дом 41,	2-ой этаж, кабинет № 202, 2-ой этаж кабинет № 207

Исполняющий обязанности
управляющего делами-руководителя
аппарата Администрации
Звериноголовского муниципального округа
Курганской области О.С. Макоклюй

Приложение 2 к распоряжению Главы Звериноголовского муниципального округа Курганской области от «31» мая 2023 года № 47-рг «Об обращении со средствами криптографической защиты информации защищенной сети передачи данных»

Инструкция о порядке доступа в спецпомещения

1. Общие положения

2.

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 года № 152 «Об утверждении Инструкции 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»;
- «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 N 378 «Об утверждении Состава и содержания 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».

1.2. Настоящая инструкция регламентируют организацию и порядок доступа в спецпомещения[1] Администрации Звериноголовского 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.

---

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

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.

Исполняющий обязанности
управляющего делами-руководителя
аппарата Администрации
Звериноголовского муниципального округа
Курганской области О.С. Макоклюй

Приложение 3 к распоряжению Главы Звериноголовского муниципального округа Курганской области от «31» мая 2023 года № 47-рг «Об обращении со средствами криптографической защиты информации 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)
1.	Администрация Звериноголовского муниципального округа Курганской области	641480, Курганская область, Звериноголовский район, село Звериноголовское, улица Чапаева, дом 41,	2-ой этаж, кабинет № 202, Металлический ящик,

Исполняющий обязанности
управляющего делами-руководителя
аппарата Администрации
Звериноголовского муниципального округа
Курганской области О.С. Макоклюй

Приложение 4 к распоряжению Главы Звериноголовского муниципального округа Курганской области от «31» мая 2023 года № 47-рг «Об обращении со средствами криптографической защиты информации защищенной сети передачи данных»

Модель нарушителя

Общие положения

1.1 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 N 378 «Об утверждении Состава и содержания 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».

1.2 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 Звериноголовского 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
1.	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
2.	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
3.	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)
4.	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
5.	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды
6.	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
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
8.	Поставщики вычислительных услуг, услуг связи	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
9.	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
10.	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
11.	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
12.	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
13.	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
1.	Отдельные физические лица (хакеры)	Внешний	Любопытство или желание самореализации (подтверждение статуса)
2.	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)
3.	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
1.	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

2.	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.
3.	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
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	Нет

	программного компонентов среды функционирования СКЗИ)	

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
1.	Проведение атаки при нахождении в пределах контролируемой зоны	актуально	-
2.	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	-
3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений, следующей информации: - сведения о физических мерах	актуально	-

	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		
4.	Использование штатных средств информационных систем, ограниченное мерами, реализованными в информационных системах, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	актуально	-
5.	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,
6.	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	
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 ПО	неактуально	
8.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационных системах, в которой используется СКЗИ, и направленными на	неактуально	

	предотвращение и пресечение несанкционированных действий		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.
9.	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	
10.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	неактуально	
11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	неактуально	
12.	Возможность воздействовать на любые компоненты СКЗИ и СФ	неактуально	

Заключительные положения

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

Исполняющий обязанности
управляющего делами-руководителя
аппарата Администрации
Звериноголовского муниципального округа
Курганской области О.С. Макоклюй

Приложение 5 к распоряжению Главы Звериноголовского муниципального округа Курганской области от «31» мая 2023 года № 47-рг «Об обращении со средствами криптографической защиты информации 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)
2.	Подсухин Александр Петрович	Начальник отдела информационных технологий Администрации Звериноголовского муниципального округа Курганской области	2-ой этаж, кабинет № 202

Исполняющий обязанности
управляющего делами-руководителя
аппарата Администрации
Звериноголовского муниципального округа
Курганской области О.С. Макоклюй

ЛИСТ СОГЛАСОВАНИЯ

к распоряжению Главы Звериноголовского муниципального округа Курганской области «Об обращении со средствами криптографической защиты информации защищенной сети передачи данных»

ПРОЕКТ ПОДГОТОВЛЕН И ВНЕСЕН:

Начальник отдела информационных технологий Администрации Звериноголовского муниципального округа Курганской области — А.П. Подсухин

ПРОЕКТ СОГЛАСОВАН:

Начальник контрольно-организационной, правовой и кадровой работы Администрации Звериноголовского муниципального округа Курганской области — О.С. Макоклюй

Главный специалист отдела контрольно-организационной, правовой и кадровой работы Администрации Звериноголовского муниципального округа Курганской области — Н.Н. Менщикова

СПРАВКА-РАССЫЛКА

к постановлению Главы Звериноголовского муниципального округа Курганской области «Об обращении со средствами криптографической защиты информации защищенной сети передачи данных»

Разослано:

1. Отдел контрольно-организационной, правовой и кадровой работы
2. Отдел информационных технологий