УТВЕРЖДАЮ

Директор

ОБУК «Госдирекция»

_____А.А. Найденов

«01» февраля 2021 г.

МП

ИНСТРУКЦИЯ

ответственного за эксплуатацию средств криптографической защиты информации

Липецк 2021

Оглавление

1. Термины, определения и сокращения

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] - состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами (Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей (Приказ ФАПСИ от 13 июня 2001 г. N 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»).

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока (Приказ ФАПСИ от 13 июня 2001 г. N 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»).

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию (Приказ ФАПСИ от 13 июня 2001 г. N 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»).

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой

информации)(Приказ ФАПСИ от 13 июня 2001 г. N 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»).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам (Приказ ФАПСИ от 13 июня 2001 г. N 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»).

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе (Приказ ФАПСИ от 13 июня 2001 г. N 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»).

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) - материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Орган криптографической защиты (ОКЗ) – организация, разрабатывающая и осуществляющая мероприятия по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа (Приказ ФАПСИ от 13 июня 2001 г. N 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»).

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для

защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

2. Общие положения

2.1. Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за организацию работ по криптографической защите информации (далее – Ответственный) в ОБУК «Госдирекция» (далее – Организация), которая осуществляет работы с применением средств криптографической защиты информации (далее - СКЗИ).

2.2. Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение автоматизированных рабочих мест пользователей государственных и муниципальных информационных систем к защищенной сети администрации Липецкой области.

2.3. Ответственный назначается приказом директора Организации из числа её работников.

2.4. СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

2.5. Функции органа криптографической защиты информации (далее – ОКЗ) для проведения мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа возложены на администрацию Липецкой области, как организатора защищенного канала связи.

2.6. Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152) и «Положении о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66.

3. Обязанности Ответственного за эксплуатацию СКЗИ

3.1. При решении всех вопросов, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом РуководителяОрганизации назначается Ответственный за эксплуатацию СКЗИ (далее-Ответственный). Ответственный должен руководствоваться Инструкцией по обращению с СКЗИ.

3.2. На Ответственного возлагается проведение следующих мероприятий:

3.2.1. ведение журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

3.2.2. ведение учета актов об установке и настройке СЗИ;

3.2.3. ведение учета лицензий на право использования СКЗИ и соответствующих им Актов приема-передачи;

3.2.4. ведение учета Пользователей СКЗИ;

3.2.5. контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;

3.2.6. расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

3.2.7. разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

3.3. Ответственный обязан:

3.3.1. не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;

3.3.2. сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

3.3.3. соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

3.3.4. контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

3.3.5. немедленно уведомлять ОКЗ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

3.3.6. незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;

3.3.7. не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

4. Права Ответственного

4.1. В рамках исполнения возложенных на него обязанностей Ответственный имеет право:

4.1.1. требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ и Инструкции пользователя СКЗИ;

4.1.2. обращаться к руководителю Организации с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

4.1.3. инициировать проведение служебных расследований по фактам нарушения в Организации порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа;

4.1.4. осуществлять текущий контроль, обеспечение функционирования и безопасность эксплуатации.

5. Обязанности пользователей СКЗИ

5.1. Пользователи СКЗИ назначаются приказом РуководителяОрганизации и допускаются к работе с СКЗИ в соответствии с разрешительной системой доступа - матрица доступа пользователей к защищаемым данным и после самостоятельного обучения правилам работы с СКЗИ. Обучение Пользователей правилам работы с СКЗИ осуществляет Ответственный за эксплуатацию СКЗИ.

5.2. Пользователь СКЗИ обязан:

5.2.1. не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;

5.2.2. соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

5.2.3. сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ;

5.2.4. незамедлительно уведомлять Ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

5.3. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения. Обучение Пользователей правилам работы с СКЗИ осуществляет Ответственный за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ должен иметь соответствующий документ о квалификации в области эксплуатации СКЗИ.

5.4. Ответственный за эксплуатацию СКЗИ и Пользователи СКЗИ должны быть ознакомлены с настоящей Инструкцией под расписку.

5.5. При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

Директор А.А. Найденов

«01» октября 2021 г.

Приложение 1

Лист ознакомления

№ п/п	Ф.И.О.	Роспись	Дата
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			