УТВЕРЖДЕНО

приказом _____

от «___» _____ 20__ года №_____

ИНСТРУКЦИЯ

Администратора безопасности средств криптографической защиты информации
ГБУЗ ЯО «_____»

Оглавление

1. Термины и определения

Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Ключевой документ – физический носитель определённой структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и техническую информацию.

Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течении определённого срока.

Ключевой носитель – физический носитель определённой структуры, предназначенный для размещения на нём ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (дискета, Smart Card, Touch Memory и т.п.).

Спецпомещения – помещения, где установлены криптосредства или хранятся ключевые документы к ним.

Пользователь СКЗИ – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Криптосредство (СКЗИ) – шифровальные (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) – шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

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.

Орган криптографической защиты (ОКЗ) – организация, разрабатывающая и осуществляющая мероприятия по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

2. Общие положения

Инструкция определяет функциональные обязанности, права и ответственность Администратора безопасности средств криптографической защиты информации (далее - СКЗИ).

Действие инструкции распространяется на сертифицированные ФСБ России СКЗИ. К ним относятся:

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при её обработке, хранении и передаче по каналам связи, включая СКЗИ;
- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при её обработке и хранении;
- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и «электронной подписи»;
- аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.

Инструкция разработана на основе нормативных правовых актов:

- «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;
- «Положения 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;
- а также эксплуатационной и технической документации на используемые в КП ЯО «Электронный регион» (далее - Предприятие) СКЗИ.

Администратор безопасности СКЗИ Предприятия и исполняющий его обязанности на время отсутствия назначаются приказом директора из числа сотрудников Предприятия и допускаются к работе только после прохождения необходимой подготовки.

Сотрудники назначаемые на должность администратора безопасности СКЗИ должны иметь высшее профессиональное образование или пройти переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами.

Администратор безопасности СКЗИ непосредственно подчиняется начальнику подразделения, в штате которого он состоит.

Исполняющий обязанности Администратора безопасности СКЗИ выполняет в отсутствии Администратора безопасности полностью его функциональные обязанности.

Функции органа криптографической защиты информации для проведения мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа возложены на отдел эксплуатации и развития ИТ инфраструктуры.

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации достигается:

- соблюдением режима конфиденциальности при обращении со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;
- точным выполнением требований к обеспечению безопасности конфиденциальной информации;
- надёжным хранением СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации;
- своевременным выявлением попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;
- немедленным принятием мер по предупреждению разглашения защищаемых сведений ограниченного доступа, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.д.

3. Обязанности администратора безопасности СКЗИ

При решении всех вопросов, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Администратор безопасности СКЗИ должен руководствоваться Инструкцией по обращению с СКЗИ, которая утверждается Приказом об обращении с СКЗИ.

На Администратора безопасности СКЗИ возлагается проведение следующих мероприятий:

1) Вести Журнал поэкземплярного учета используемых и хранимых СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
2) Вести учёт обслуживаемых клиентов Предприятия – обладателей конфиденциальной информации, а также сотрудников Предприятия, непосредственно допущенных к работе с СКЗИ (далее – пользователи СКЗИ);
3) Подача заявок ОКЗ на изготовление ключевых документов к СКЗИ, или исходной ключевой информации. Изготовление из исходной ключевой информации ключевых документов, их распределение, рассылка и учёт;
4) Вести учет переданных от ОКЗ актов об установке и настройке СЗИ;
5) Вести учет переданных от ОКЗ лицензий на право использования СКЗИ и соответствующих им Актов приема-передачи;
6) Принять СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

7) Сообщать в ОКЗ о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
8) Проводить обучение пользователей СКЗИ, правилам работы с ними;
9) Проводить мероприятия по обеспечению штатного функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам, нормативно-методическими документами ФАПСИ, ФСБ России и внутренними нормативно-методическими документами Предприятия.
10) Разработка схемы организации криптографической защиты информации (с указанием обладателей конфиденциальной информации, реквизитов договоров на оказание услуг по криптографической защите конфиденциальной информации, а также с указанием типов применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения и средств вычислительной техники). Указанная схема согласуется с ОКЗ и утверждается директором.

Ответственный обязан:

1) Не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;
2) Сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
3) Соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
4) Контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;
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;
6) Незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера.

4. Права администратора безопасности СКЗИ

Администратор безопасности СКЗИ Предприятия имеет право:

- требовать от пользователей СКЗИ безусловного соблюдения установленных правил организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации с использованием средств криптографической защиты;
- инициировать обращение к руководителю Предприятия с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;

- инициировать проведение служебных расследований по фактам нарушения на предприятии порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа;
- обращаться в ОКЗ Предприятия с просьбой об оказании технической и методической помощи в работе по обеспечению безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации с использованием средств криптографической защиты информации.

5. Ответственность администратора безопасности СКЗИ

На Администратора безопасности СКЗИ возлагается персональная ответственность за строгое и точное выполнение возложенных на него обязанностей по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации с использованием средств криптографической защиты информации.

Администратор безопасности СКЗИ несёт персональную ответственность за сохранность конфиденциальной ключевой информации от несанкционированного доступа посторонних лиц.

Лист ознакомления

с Инструкцией администратора безопасности средств криптографической защиты информации ГБУЗ ЯО «_____»

(утверждена приказом от «___»_____ 20___ г. № _____)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата