Вопросы криптографической защиты информации в образовательных организациях

Консультант отдела реализации государственных программ, информационных технологий министерства образования Кировской области
Захарова Дарья Алексеевна

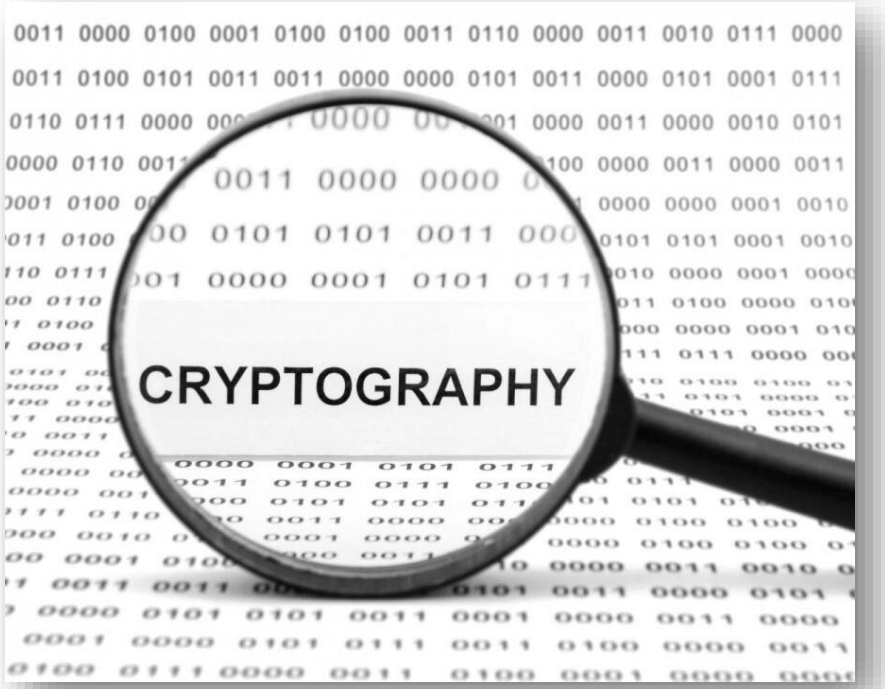
Ведущий инженер-программист отдела цифровых образовательных технологий и информационной политики КОГОАУ ДПО «ИРО Кировской области»
Кряжевских Александр Владимирович

Криптографические средства защиты информации

это средства защиты информации, реализующие алгоритмы криптографического преобразования информации с использованием специальных аппаратных и программных средств

Цель использования:

1. Сохранение конфиденциальности информации при её передаче по сетям связи, информационно-телекоммуникационным сетям;
2. Обеспечение целостности информации;
3. Обеспечение подлинности и юридической значимости электронных документов;
4. Защита парольных систем в автоматизированных системах.



Методика проведения самообследования (аудита) процессов обработки персональных данных образовательной организации

«Технические меры и криптография»

Раздел 3.5 (13 контрольных точек)

!

№№	Перечень шаблонов локальных актов
1	**Приказ об обеспечении безопасности персональных данных с использованием СКЗИ**
2.	**Инструкция по обращению с СКЗИ**
2.1	Приложение 1 - ЖУРНАЛ учета СЗИ_СКЗИ
2.2	Приложение 2 - ЖУРНАЛ замечаний по контролю СКЗИ
3	**Инструкция пользователя СКЗИ**
4.	**Приказ о допуске пользователей СКЗИ**

Нормативно-правовые требования

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
- Приказ ФСБ России от 10.07.2014 № 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».
- Приказ ФАПСИ от 13.06.2001 № 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».

Приказ ФСБ РФ от 9 февраля 2005 г. № 66 (Положение ПКЗ-2005)»

Средствами криптографической защиты информации в положении именуются **шифровальные (криптографические) средства защиты информации конфиденциального характера**.

К СКЗИ относятся:

а) **средства шифрования** (например, ViPNet Client, Континент-АП, ПАК ViPNet HW100, HW1000).

б) **средства имитозащиты** (например, использование HMAC на основе хэш-функций ГОСТ Р 34.11-94/ГОСТ Р 34.11-2012).

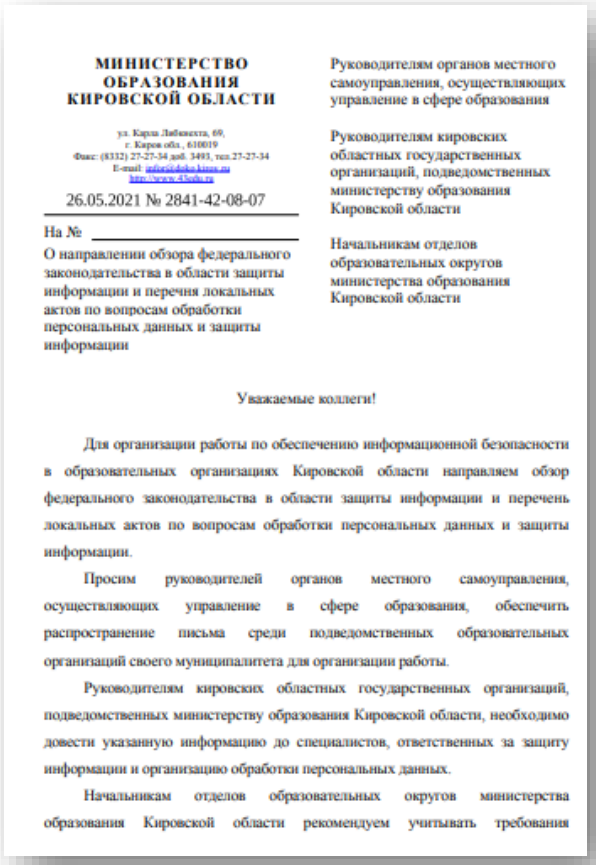
в) **средства электронной цифровой подписи** (например, ViPNet CSP, КриптоПРО CSP, КриптоАРМ, ViPNet PKI Client).

г) **средства кодирования** (например, азбука Морзе, флажковая азбука).

д) **средства изготовления ключевых документов** (независимо от вида носителя ключевой информации). Используются удостоверяющими центрами.

е) **ключевые документы** (независимо от вида носителя ключевой информации), то есть документы, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации, записанные на носителе (например, сертификаты электронной подписи).

Приказ ФСБ России от 10.07.2014 № 378



МИНИСТЕРСТВО ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ

ул. Карла Либкнехта, 69,
г. Киров обл., 610019
Факс: (8332) 27-27-34 доб. 3493, тел.27-27-34
E-mail: info@doka.kirov.ru
http://www.43edu.ru

26.05.2021 № 2841-42-08-07

На № _____

О направлении обзора федерального законодательства в области защиты информации и перечня локальных актов по вопросам обработки персональных данных и защиты информации

Руководителям органов местного самоуправления, осуществляющих управление в сфере образования

Руководителям кировских областных государственных организаций, подведомственных министерству образования Кировской области

Начальникам отделов образовательных округов министерства образования Кировской области

Уважаемые коллеги!

Для организации работы по обеспечению информационной безопасности в образовательных организациях Кировской области направляем обзор федерального законодательства в области защиты информации и перечень локальных актов по вопросам обработки персональных данных и защиты информации.

Просим руководителей органов местного самоуправления, осуществляющих управление в сфере образования, обеспечить распространение письма среди подведомственных образовательных организаций своего муниципалитета для организации работы.

Руководителям кировских областных государственных организаций, подведомственных министерству образования Кировской области, необходимо довести указанную информацию до специалистов, ответственных за защиту информации и организацию обработки персональных данных.

Начальникам отделов образовательных округов министерства образования Кировской области рекомендуем учитывать требования

ОБЗОР ФЕДЕРАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Любая эксплуатация СКЗИ должна осуществляться в соответствии с документацией на СКЗИ и нормативно-правовыми актами, регламентирующими отношения в данной области.

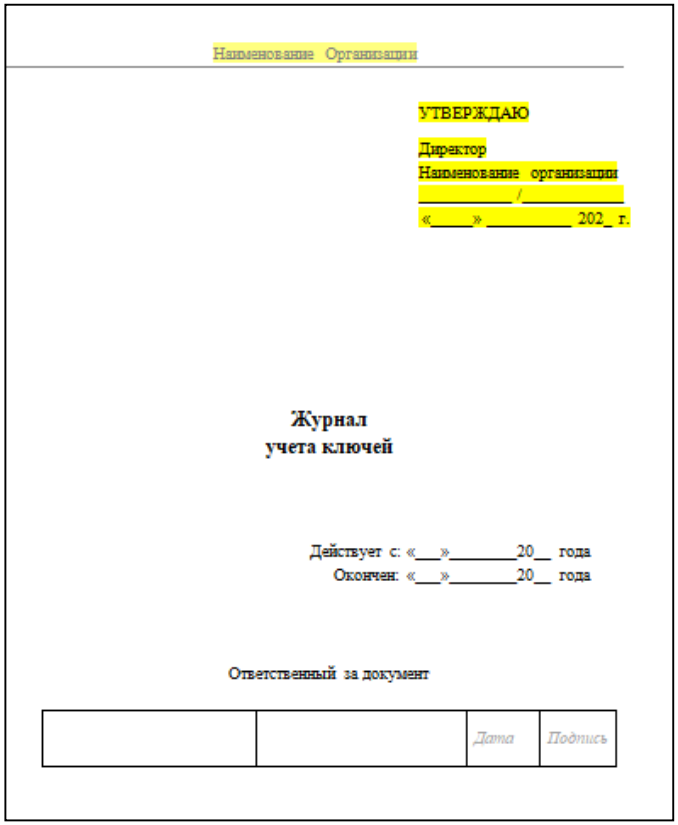
Состав и содержание организационных и технических мер, необходимых для выполнения установленных требований криптографической защиты в информационных системах персональных данных **зависит от уровня защищенности персональных данных.**

Требования по определению уровней защищенности установлены постановлением Правительства Российской Федерации от 01.11.2012 № 1119
(для образовательных организаций актуальны требования установленные для 4 и 3 уровней защищенности)

Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

Достигается путем:

1) Оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода. Ключи, пломбы, печати от помещений и сейфов должны быть учтены в журнале (Раздел 2 направленных шаблонов: Режимные меры).
2) Утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
3) Утверждения перечня лиц, имеющих право доступа в Помещения.



Наименование Организации

УТВЕРЖДАЮ

Директор
Наименование организации
_____/_____
«____» _____ 202_ г.

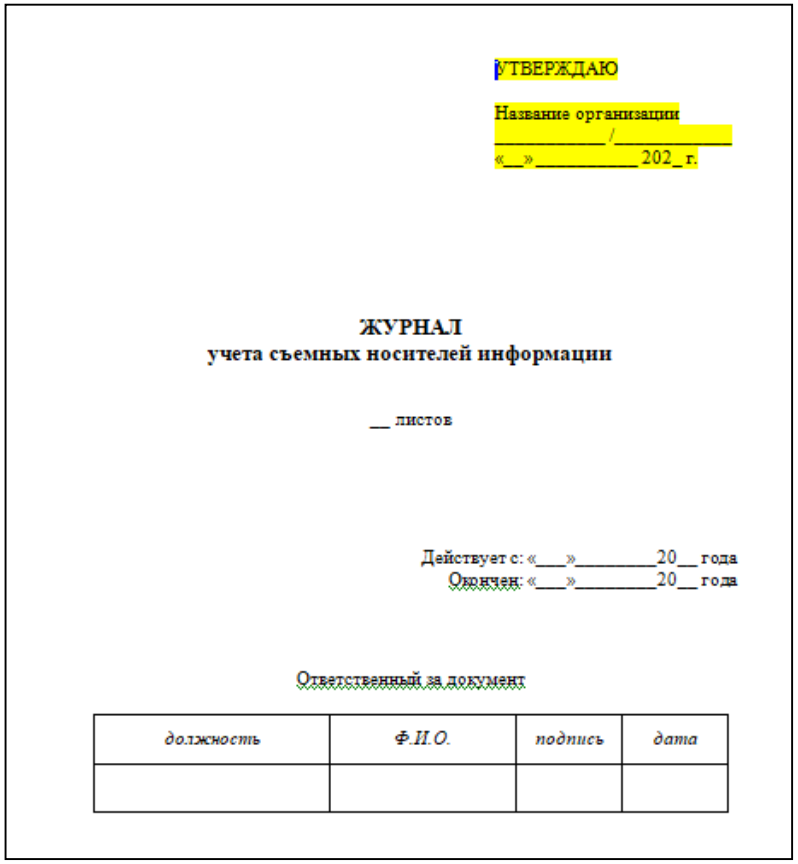
Журнал
учета ключей

Действует с: «___»_____20__ года
Окончен: «___»_____20__ года

Ответственный за документ

		Дата	*Подпись*

Обеспечение сохранности носителей персональных данных



УТВЕРЖДАЮ

Название организации
_____/_____
«__»_____202_г.

ЖУРНАЛ
учета съемных носителей информации

__ листов

Действует с: «___»_____20__ года
Окончен: «___»_____20__ года

Ответственный за документ

должность	*Ф.И.О.*	*подпись*	*дата*

Достигается путем:

1) Осуществления хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.

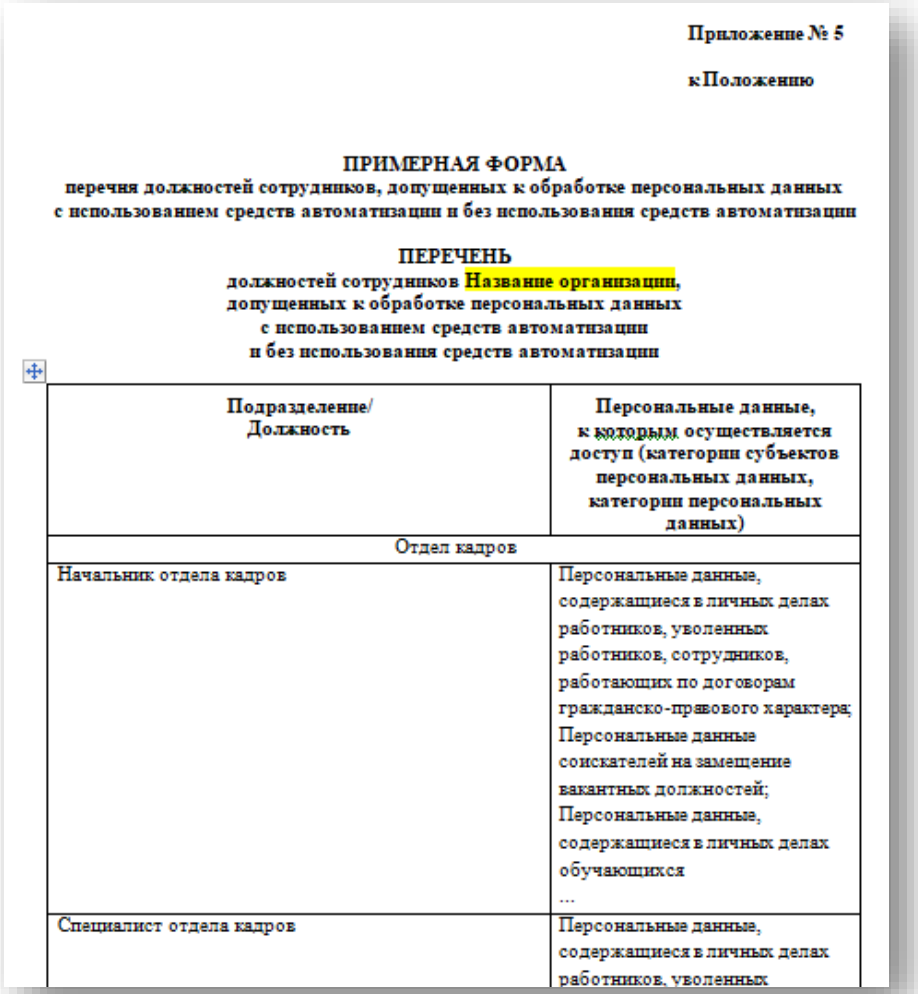
2) Осуществления поэкземплярного учета машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.

Утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей

Разработан

Утвержден

Поддерживается в актуальном состоянии



Приложение № 5

к Положению

ПРИМЕРНАЯ ФОРМА
перечня должностей сотрудников, допущенных к обработке персональных данных с использованием средств автоматизации и без использования средств автоматизации

ПЕРЕЧЕНЬ
должностей сотрудников Название организации, допущенных к обработке персональных данных с использованием средств автоматизации и без использования средств автоматизации

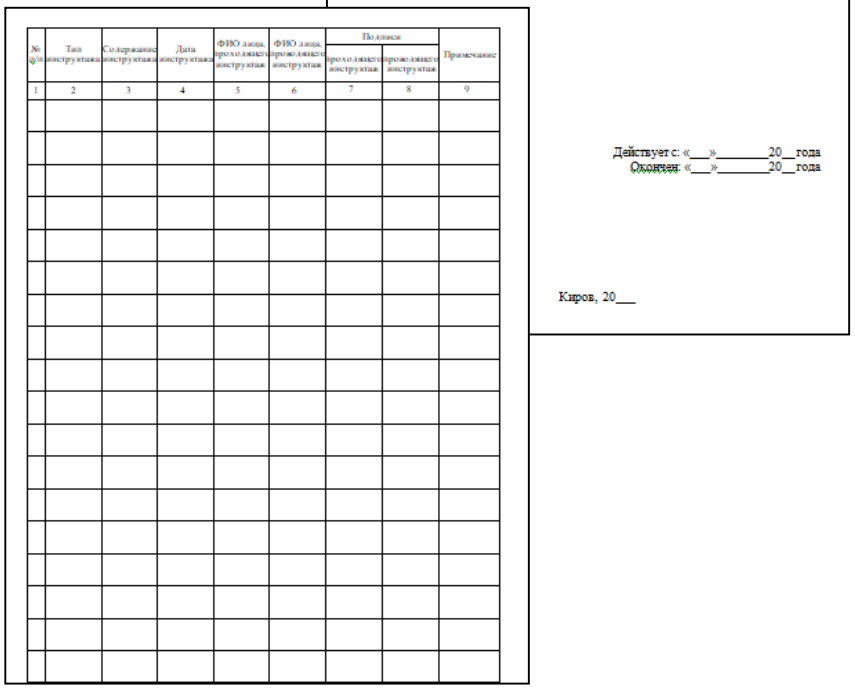
Подразделение/ Должность	Персональные данные, к которым осуществляется доступ (категории субъектов персональных данных, категории персональных данных)
Отдел кадров	
Начальник отдела кадров	Персональные данные, содержащиеся в личных делах работников, уволенных работников, сотрудников, работающих по договорам гражданско-правового характера; Персональные данные соискателей на замещение вакантных должностей; Персональные данные, содержащиеся в личных делах обучающихся ...
Специалист отдела кадров	Персональные данные, содержащиеся в личных делах работников, уволенных

Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

Использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ определенного класса

Уровень защищенности ПДн	4 УЗ	3 УЗ		2 УЗ			1 УЗ	
Тип актуальных угроз	3	2	3	1	2	3	1	2
Минимальный класс СКЗИ	КС1	КВ	КС1	КА	КВ	КС1	КА	КВ

Приказ Федерального агентства правительственной связи и информации при президенте Российской Федерации (ФАПСИ) от 13.06.2001 № 152



Наименование организации

УТВЕРЖДАЮ

Название организации
_____/_____
«__»_____202_г.

ЖУРНАЛ

инструктажа по вопросам информационной безопасности

Действует с: «___»_____20__года
Окончен: «___»_____20__года

Киров, 20___

№ п/п	Тип инструктажа	Содержание инструктажа	Дата инструктажа	ФИО лица, проводившего инструктаж	ФИО лица, прошедшего инструктаж	Подписи		Примечание
						прошедшего инструктаж	проводившего инструктаж	
1	2	3	4	5	6	7	8	9

Пункт 19	Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.
Пункт 20	Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Приказ Федерального агентства правительственной связи и информации при президенте Российской Федерации (ФАПСИ) от 13.06.2001 № 152

Должны быть разработаны и утверждены локальным актом организации **следующие документы:**

1) Инструкция по эксплуатации СКЗИ. Данная инструкция предназначена для ответственного за СКЗИ, администратора СКЗИ.
2) Инструкция пользователя СКЗИ. Данная инструкция предназначена для пользователей СКЗИ и содержит только необходимые пользователям условия и требования.

Приказ Федерального агентства правительственной связи и информации при президенте Российской Федерации (ФАПСИ) от 13.06.2001 № 152

Используемые или хранимые средства криптографической защиты информации (далее – СКЗИ), эксплуатационная и техническая документация к ним, ключевые документы **подлежат поэкземплярному учету.**
(Пункты 26-27 Инструкции)

В каждой организации должно быть обеспечено:
✓Наличие журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.
✓Наличие журнала учета ключевых носителей.

Учитываются следующие экземпляры СКЗИ:
лицензии на программное обеспечение (аппаратные средства, программно-аппаратные средства), дистрибутивы, ключевые носители, ключевые документы, формуляры, сертификаты электронной подписи

Журнал учета СЗИ/СКЗИ, эксплуатационной и технической документации к ним

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены или Ф.И.О. сотрудника ОКЗ, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Ф.И.О пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников ОКЗ, пользователя СКЗИ*, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников ОКЗ, пользователя СКЗИ*, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Диск CD-ROM с дистрибутивом СКЗИ	Инв.№ 5421	1	ООО «Компания»	т/н № 44313 от 22.02.2020	Леонов Сергей Павлович	Акт приема передачи №22 от 13.02.2020							
2	Серийный номер лицензии КриптоПро CSP	HR9J-EEWR-45W3-VL4Q-842Q	1	ООО «Компания»	т/н № 44313 от 22.02.2020	Хрусталева Ирина Валерьевна	Акт приема передачи № 55 от 30.07.2020	Хрусталева Ирина Валерьевна	30.07.2020	442234	20.09.2020	Леонов Сергей Павлович	Акт об изъятии СКЗИ № 5 От 20.09.2020	
3	Серийный номер лицензии КриптоПро CSP	4454-NG96-8421-6401-WQRG	1	ООО «Компания»	т/н № 44313 от 22.02.2020	Иванов Иван Иванович	Акт приема передачи № 43 от 25.07.2020	Иванов Иван Иванович	27.07.2020	756745GR	30.08.2020	Леонов Сергей Павлович	Акт об изъятии СКЗИ № 58 от 30.08.2020	
4	Серийный номер лицензии КриптоПро CSP	34DR-4231-4123-0003-1200	1	ООО «Компания»	т/н № 44313 от 22.02.2020	Груздев Сергей Леонидович	Акт приема передачи № 2 от 01.09.2020	Леонов Сергей Павлович	10.09.2020	541GGBN	17.12.2020	Леонов Сергей Павлович	Акт об изъятии СКЗИ № 43 от 30.11.2020	
5	Формуляр СКЗИ «КриптоПро CSP» версии 4.2	ЖТЯИ.00002-02 30 10	1	ООО «Компания»	т/н № 44313 от 22.02.2020									

Журнал учета ключевых носителей информации

В журнал вы заносите следующую информацию:

1.Номер носителя;

2.Отметку о выдаче носителя;
(ФИО пользователя, дату, подпись пользователя);

3.Отметку о возвращении носителя
(дату возвращения, ФИО пользователя, подпись администратора СКЗИ);

4.Можно указывать примечания.

№¶ п/п	Номер ключевого носителя¶	Отметка о выдаче			Отметка о возвращении			Примечание
		Ф.И.О.¶ пользователя	Дата	Подпись	Дата возвращения	Ф.И.О. пользователя¶	Подпись	

Наименование организации

УТВЕРЖДАЮ
_____
_____
_____/_____
от «___»_____202__года

ЖУРНАЛ
учета ключевых носителей

Действует с: «___»_____20__года
Окончен: «___»_____20__года

Лицо, ответственное за ведение журнала:

Должность	Подпись	ФИО

Киров, 202_

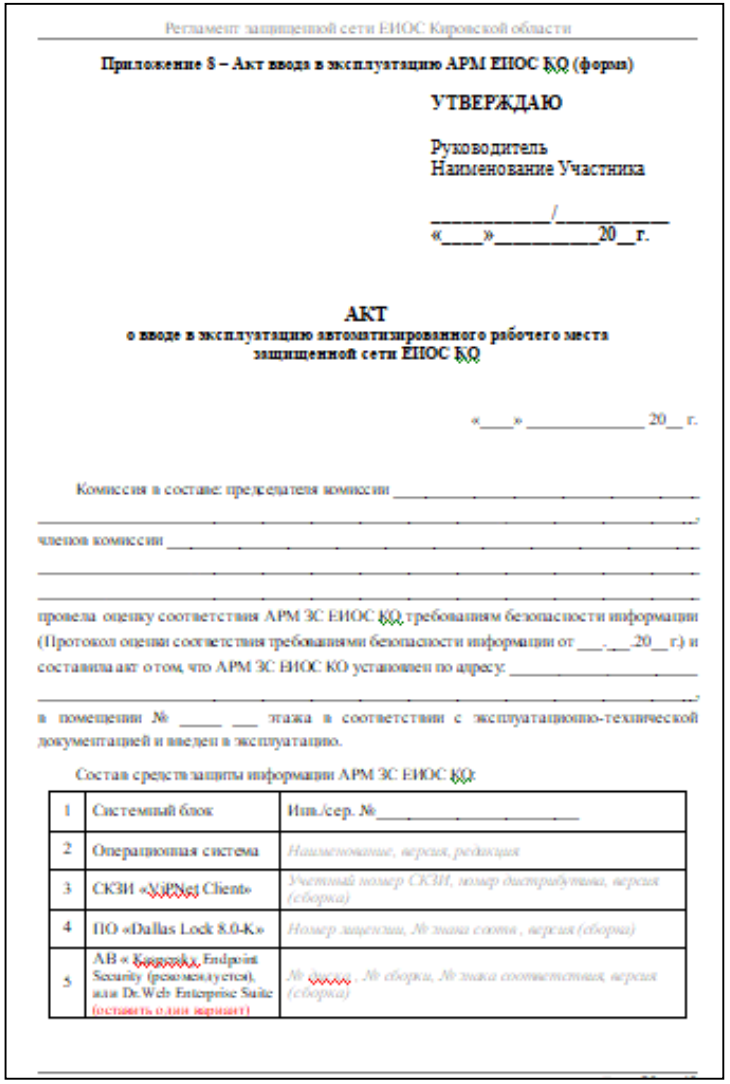
Режимные меры хранения и эксплуатации СКЗИ

Пункты 30,64,66	Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
Пункт 31	Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно - программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).

Размещение и монтаж СКЗИ (Пункт 62)

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

СКЗИ должны быть введены в эксплуатацию принятием акта о вводе в эксплуатацию!



Регламент защищенной сети ЕИОС Кировской области

Приложение 8 – Акт ввода в эксплуатацию АРМ ЕИОС КО (форм)

УТВЕРЖДАЮ

Руководитель
Наименование Участника

_____/_____
«____»_____20__г.

АКТ
о вводе в эксплуатацию автоматизированного рабочего места защищенной сети ЕИОС КО

«____» _____ 20__ г.

Комиссия в составе: председателя комиссии _____,
_____,
членов комиссии _____,
_____,
_____,
провела оценку соответствия АРМ ЗС ЕИОС КО требованиям безопасности информации (Протокол оценки соответствия требованиям безопасности информации от ___.___20__г.) и составила акт о том, что АРМ ЗС ЕИОС КО установлен по адресу: _____,
_____,
в помещении № _____ ___ этажа в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию.

Состав средств защиты информации АРМ ЗС ЕИОС КО:

1	Системный блок	Инв./сер. №_____
2	Операционная система	*Наименование, версия, редакция*
3	СКЗИ «ViPNet Client»	*Учетный номер СКЗИ, номер дистрибутива, версия (сборка)*
4	ПО «Dallas Lock 8.0-K»	*Номер лицензии, № знака соотв., версия (сборка)*
5	АВ «Kaspersky Endpoint Security (рекомендуется), или Dr.Web Enterprise Suite (оставить один вариант)	*№ диска, № сборки, № знака соответствия, версия (сборка)*

Вывод из эксплуатации СКЗИ и их уничтожение (пункты 42, 47 Инструкции)

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Например:
«Удаление СКЗИ произведено с использованием механизма гарантированного удаления остаточной информации в составе утилиты clean.exe версии 2.1 производства ОАО «ИнфоТеКС», количество циклов затирания – 3».

Учет уничтожения:

- разовое фиксируется в журнале учета лицом, ответственным за СКЗИ;
- уничтожение нескольких ключей, ключевых документов фиксируется по акту уничтожения.

Ежегодный контроль эксплуатации СКЗИ

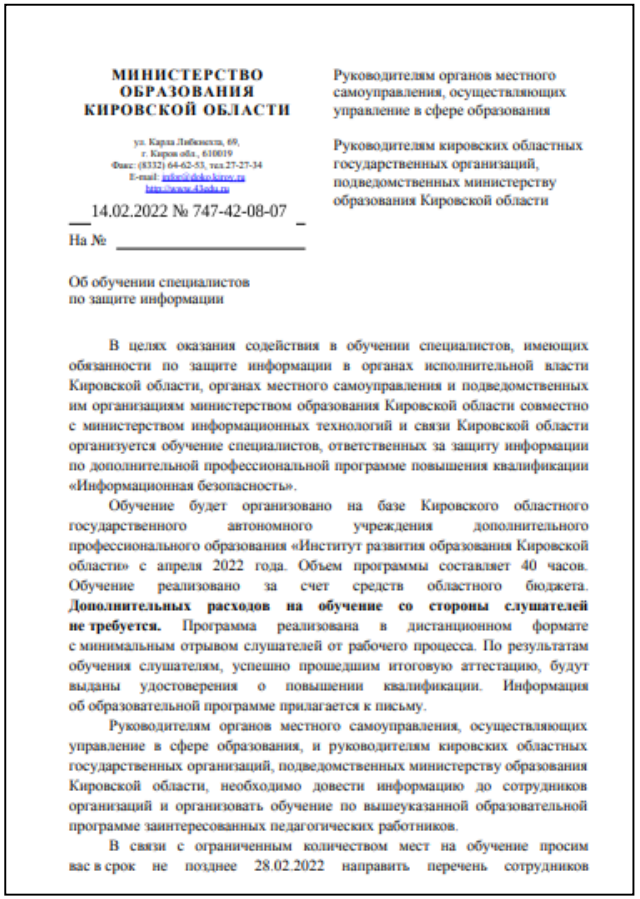
№ п/п	Вид контроля (плановый/ внеплановый)	Дата	ФИО контролирующего	Замечания по результатам контроля, подпись контролирующего	Дата устранения замечания, подпись Администратора СКЗИ
1	2	3	4	5	6
1.	Плановый	01.09.20	Иванов И.И.	Контроль пройден	администратор СКЗИ
				без замечаний	
				Иванов И.И.	Петров П.П.
2.	Плановый	01.09.21	Иванов И.И.	По результатам контроля	
				выявлены замечания:	
				1. Не опечатывается	05.09.21 устранено
				сейф для хранения СКЗИ	Петров П.П.
				2. Возврат ключа	13.09.21 устранено
				Корольковой И.А. на	Петров П.П.
				время отпуска не учтен	

Ответственность

13.12 КоАП РФ	**Нарушение правил защиты информации, в том числе:** **Часть 2.** Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), **Часть 6.** Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	149-ФЗ, 152-ФЗ, 63-ФЗ	Штраф: - Долж.лица:1-2 т.р. - Юр.лица: 15-20 т.р.

Обучение специалистов по защите информации

Письмо министерства образования Кировской области от 14.02.2022 № 747-42-08-07



МИНИСТЕРСТВО ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ

ул. Карла Либкнехта, 69,
г. Киров обл., 610019
Факс: (8332) 64-62-53, тел.27-27-34
E-mail: info@doko.kirov.ru
http://www.43edu.ru

14.02.2022 № 747-42-08-07

На № _____

Руководителям органов местного самоуправления, осуществляющих управление в сфере образования

Руководителям кировских областных государственных организаций, подведомственных министерству образования Кировской области

Об обучении специалистов по защите информации

В целях оказания содействия в обучении специалистов, имеющих обязанности по защите информации в органах исполнительной власти Кировской области, органах местного самоуправления и подведомственных им организациям министерством образования Кировской области совместно с министерством информационных технологий и связи Кировской области организуется обучение специалистов, ответственных за защиту информации по дополнительной профессиональной программе повышения квалификации «Информационная безопасность».

Обучение будет организовано на базе Кировского областного государственного автономного учреждения дополнительного профессионального образования «Институт развития образования Кировской области» с апреля 2022 года. Объем программы составляет 40 часов. Обучение реализовано за счет средств областного бюджета. **Дополнительных расходов на обучение со стороны слушателей не требуется.** Программа реализована в дистанционном формате с минимальным отрывом слушателей от рабочего процесса. По результатам обучения слушателям, успешно прошедшим итоговую аттестацию, будут выданы удостоверения о повышении квалификации. Информация об образовательной программе прилагается к письму.

Руководителям органов местного самоуправления, осуществляющих управление в сфере образования, и руководителям кировских областных государственных организаций, подведомственных министерству образования Кировской области, необходимо довести информацию до сотрудников организаций и организовать обучение по вышеуказанной образовательной программе заинтересованных педагогических работников.

В связи с ограниченным количеством мест на обучение просим вас в срок не позднее 28.02.2022 направить перечень сотрудников

Программа повышения квалификации по направлению «Информационная безопасность», 40 часов

Программа реализуется на базе КОГОАУ ДПО «ИРО Кировской области»

Направить заявку посредством заполнения формы, расположенной в информационно-телекоммуникационной сети «Интернет» по адресу: https://forms.yandex.ru/cloud/6204deeb867508c4b007115d/ **до 28.02.2022**.

СПАСИБО ЗА ВНИМАНИЕ!

Захарова Дарья Алексеевна,
консультант отдела реализации государственных программ, информационных технологий министерства образования Кировской области

тел. 8 (8332) 27-27-34, доб. 34-64
zakharova.da@ako.kirov.ru

Кряжевских Александр Владимирович,
ведущий инженер-программист отдела цифровых образовательных технологий и информационной политики КОГОАУ ДПО «ИРО Кировской области»

av.kryazhevskih@kirovipk.ru