ИНСТИТУТ
развития образования
1887
города Севастополь

Государственное автономное образовательное учреждение профессионального образования города Севастополя «Институт развития образования»
(ГАОУ ПО ИРО)

# П Р И К А З

«05» ноября 2024 г. № 819

Об утверждении инструкций и назначении ответственных

С целью систематизации и актуализации регламентирующих документов, приведения деятельности ГАОУ ПО «Институт развития образования» в соответствие с требованиями Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» в сфере защиты информации, персональных данных и иной конфиденциальной информации, **приказываю:**

1. Изложить в новой редакции, утвердить и ввести в действие следующие нормативно-правовые и распорядительные акты:

1.1. Инструкция ответственного за организацию обработки персональных данных в ГАОУ ПО «Институт развития образования». (Приложение № 1).

1.2. Инструкция ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в ГАОУ ПО «Институт развития образования». (Приложение № 2).

1.3. Правила доступа работников в помещения ГАОУ ПО «Институт развития образования», где осуществляется хранение и эксплуатация СКЗИ в рабочее и нерабочее время, а также в нештатных ситуациях. (Приложение № 3).

1.4. Правила, цель и способы обработки персональных данных в ФИС «ГИА и Приема» (Приложение № 4).

1.5. Перечень должностных лиц и работников ГАОУ ПО «Институт развития образования», имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ФИС «ГИА и Приема» (Приложение № 5).

1.6. Матрица доступа к защищаемым информационным ресурсам ФИС «ГИА и Приема» (Приложение № 6).

1.7. Правила осуществления в ГАОУ ПО «Институт развития образования» внутреннего контроля соответствия обработки персональных данных требованиям, предъявляемым к защите персональных данных (Приложение № 7).

1.8. Перечень мест использования и хранения съёмных носителей персональных данных, информации ограниченного доступа и иной конфиденциальной информации (Приложение № 8).

1.9. Инструкция о порядке учета, хранения и использования съемных носителей ключевой информации в ГАОУ ПО «Институт развития образования» (Приложение № 9).

1.10. Форма обязательства о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну (Приложение № 10).

1.11. Инструкция ответственного за обеспечение безопасности персональных данных в ГАОУ ПО «Институт развития образования» (Приложение № 11).

1.12. Инструкция о порядке технического обслуживания, ремонта, модернизации технических и программных средств, средств защиты информации, входящих в состав информационных систем обработки персональных данных ГАОУ ПО «Институт развития образования» (Приложение № 12).

1.13. Положение по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации ГАОУ ПО «Институт развития образования». (Приложение № 13).

2. Считать утратившими силу приказы ГАОУ ПО ИРО: № 352 от 24.04.2023, № 354 от 24.04.2023, № 355 от 24.04.2023, № 356 от 24.04.2023, № 357 от 24.04.2023, № 736 от 29.09.2023, № 738 от 29.09.2023, № 750 от 02.10.2023, № 751 от 02.10.2023, № 753 от 02.10.2023, № 910 от 03.11.2023, № 911 от 03.11.2023, № 976 от 03.11.2023, № 89 от 09.02.2024, № 154 от 27.02.2024, № 200 от 11.03.2024.

3. Дальнейшие мероприятия в сфере защиты персональных данных и иной конфиденциальной информации проводить в соответствии с требованиями настоящего приказа, а также в соответствии с приказами ГАОУ ПО ИРО от 06.02.2024 г. № 82 «Об организации мероприятий по обеспечению защиты персональных данных и иной конфиденциальной информации в ГАОУ ПО ИРО», от 22.07.2024 г. № 516 «О назначении ответственных лиц», от 05.09.2024 г. № 604 «О назначении должностных лиц, ответственных за организацию работы в сфере обработки персональных данных и иной конфиденциальной информации».

4. Назначить ответственным за общее руководство и организацию работ по защите информации и персональных данных в ГАОУ ПО ИРО начальника Центра информационно-программного обеспечения ГАОУ ПО ИРО Гладких И.Ю.

5. Назначить специалистом, ответственным за защиту информации и ответственным пользователем средств криптографической защиты информации (далее - СКЗИ) в ГАОУ ПО ИРО – главного специалиста по защите информации Центра информационно-программного обеспечения ГАОУ ПО ИРО Дементьева А.В.

6. Центру кадрового учета, документооборота и канцелярии довести требования данного приказа всем названным лицам. В случае их отсутствия (временная нетрудоспособность, отпуск, командировка и т.д.) – в день выхода на работу.

7. Начальнику Центра информационно-программного обеспечения ГАОУ ПО ИРО Гладких И.Ю. разместить данный приказ на официальном сайте ГАОУ ПО ИРО.

9. Контроль за выполнением требований приказа возложить на заместителя директора по безопасности и финансово-экономической деятельности Котельникова Д.В.

Директор Е.И. Миргород

**ПРОЕКТ ПРИКАЗА ПОДГОТОВИЛ:**
Заместитель директора по безопасности
и финансово-экономической деятельности
_____ Д.В. Котельников
«__» ноября 2024 г.

**СОГЛАСОВАНО:**
Начальник Центра информационно-
программного обеспечения
_____ И.Ю. Гладких
«05» ноября 2024 г.

**ОЗНАКОМЛЕНЫ:**

| Должность | Фамилия И.О. | Подпись | Дата |
|---|---|---|---|
| Заместитель директора | Котельников Д.В. | | |
| Начальник Центра информационно-программного обеспечения | Гладких И.Ю. | | 07.11.2024 |
| Начальник Центра кадрового учета, документооборота и канцелярии | Коптенко Е.И. | | 07.11.2024 |
| Главный специалист по защите информации | Дементьев А.В. | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Приложение № 2
к приказу ГАОУ ПО ИРО
№ 819 от 05.11.2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ИНСТРУКЦИЯ

## ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных ГАОУ ПО «Институт развития образования»

**г. Севастополь - 2024**

Приложение № 1
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ИНСТРУКЦИЯ
## ответственного за организацию обработки персональных данных ГАОУ ПО «Институт развития образования»

**г. Севастополь - 2024**

# ИНСТРУКЦИЯ
**ответственного за организацию обработки персональных данных при их обработке в информационных системах персональных данных ГАОУ ПО «Институт развития образования»**

## 1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и определяет обязанности, ответственность и права ответственного за организацию обработки персональных данных в ГАОУ ПО ИРО.

1.2. Ответственный за организацию обработки персональных данных назначается приказом руководителя ГАОУ ПО ИРО.

## 2. Обязанности

2.1 К функциональным обязанностям ответственного за организацию обработки персональных данных относится:

- организация работ по обработке персональных данных в информационных системах ГАОУ ПО ИРО;
- представление руководству отчетов о состоянии защиты персональных данных, обрабатываемых в информационных системах персональных данных;
- участие в составе комиссии при проведении служебных проверок по фактам нарушений требований по обеспечению безопасности персональных данных;
- оперативное принятие мер по пресечению нарушений требований по обеспечению безопасности персональных данных;
- по требованию руководителя ГАОУ ПО ИРО предоставлять отчеты о мероприятиях и результатах работы по обеспечению безопасности персональных данных.

## 3. Ответственность

3.1. Ответственный за организацию обработки персональных данных несет ответственность за:

- неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей Инструкцией;
- совершенные в процессе осуществления своей деятельности правонарушения, которые несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, предусмотренном законодательством Российской Федерации.

## 4. Права

4.1. Ответственный за организацию обработки персональных данных имеет право:

- получать сведения об актуальном состоянии защиты персональных данных, обрабатываемых в информационных системах персональных данных;
- требовать прекращения обработки персональных данных в случае выявления нарушений требований по обработке и обеспечению безопасности персональных данных.

# ИНСТРУКЦИЯ
## ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах ГАОУ ПО «Институт развития образования»

### 1. Общие положения

1.1 Инструкция является локальным правовым актом, регламентирующим деятельность должностного лица, ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах ГАОУ ПО ИРО (далее – Ответственное лицо).

1.2 Целью настоящей Инструкции является регламентирование работы должностного лица, ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах ГАОУ ПО ИРО и обеспечения безопасности информации в используемых информационных системах персональных данных Оператора.

1.3 Назначение Ответственного лица, закрепление за ним определенных полномочий и обязанностей производится приказом руководителя ГАОУ ПО ИРО.

1.4 Ответственное лицо должно знать и применять в своей повседневной деятельности:

- законодательные акты, нормативные и методические материалы по вопросам, связанным с обеспечением защиты ПДн;
- структуру ИСПДн и особенности обработки ПДн;
- функции системы защиты персональных данных (далее СЗПДн);
- документацию на используемые в СЗПДн средства защиты информации;
- методы и средства контроля эффективности защиты ПДн;
- методы планирования и организации проведения работ по защите ПДн;
- технические средства контроля и защиты информации, перспективы и направления их совершенствования.

### 2. Основные функции Ответственного лица

2.1 Обеспечение устойчивой работоспособности и безопасности ИСПДн в соответствии с нормативными правовыми актами, локальными актами по вопросам обработки и защиты персональных данных.

2.2 Организация работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в ИСПДн, а также правильность использования и штатного функционирования средств защиты информации.

### 3. Обязанности Ответственного лица.

Ответственный за обеспечение безопасности персональных данных обязан:

3.1. Организовывать выполнение мероприятий:

- по предоставлению и разграничению доступа в информационные системы персональных данных;
- по закрытию технических каналов утечки персональных данных, при их наличии;

• по защите от несанкционированного доступа к персональным данным;

• по выбору средств защиты персональных данных;

• по своевременному обнаружению фактов несанкционированного доступа к персональным данным, обрабатываемым в ИСПДн;

•по недопущению воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование;

•по обеспечению возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

•по обеспечению хранения двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности.

3.2. Осуществлять постоянный контроль за обеспечением уровня защищенности персональных данных, при их обработке в ИСПДн.

3.3. Проводить внутренние проверки состояния технической защиты персональных данных не менее двух раз в год.

3.4. Определять события безопасности, подлежащие регистрации, и сроки их хранения, а также состава и содержания информации о событиях безопасности, подлежащих регистрации.

3.5. Осуществлять контроль за соблюдением условий использования средств защиты информации (в том числе криптографических), предусмотренных эксплуатационной и технической документацией.

3.6. Вести поэкземплярный учет носителей персональных данных, применяемых средств защиты (в том числе криптографических), а также эксплуатационной и технической документации к ним.

3.7. Готовить отчеты о состоянии работ по обеспечения технической защиты персональных данных.

3.8. Осуществлять текущий и периодический контроль работоспособности средств и систем защиты ПДн.

3.9. Осуществлять планирование и проведение мероприятий по антивирусной защите.

3.10. Поддерживать непрерывность функционирования системы защиты персональных данных.

3.11. Проводить ознакомление пользователей ИСПДн с правилами работы со средствами защиты информации.

3.12. Участвовать в подготовке объектов Оператора к аттестации по выполнению требований обеспечения безопасности персональных данных, в случае принятия руководством Оператора решения о необходимости проведения аттестации.

3.13. Участвовать в проводимых работах по совершенствованию системы защиты персональных данных.

3.14. Участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой ПДн, попыток несанкционированного доступа в ИСПДн, несоблюдения правил и условий работы в ИСПДн, хранения носителей персональных данных, использования средств защиты информации (в том числе криптографических) и иных нарушений, снижающих уровень защищенности персональных данных, разработка предложений

по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

3.15. Информировать лицо, ответственное за обеспечение безопасности персональных данных о фактах нарушения установленного порядка работ, попытках несанкционированного доступа к информационным ресурсам ИСПДн, действиях сотрудников, нарушающих установленные требования к обеспечению безопасности персональных данных.

**4. Права Ответственного лица.**

Ответственный за обеспечение безопасности персональных данных имеет право:

4.1. Вносить свои предложения по совершенствованию мер защиты персональных данных.

4.2. Ходатайствовать перед руководством ГАОУ ПО ИРО о прекращении обработки информации, как в целом в ИСПДн, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн.

4.3. Обращаться к лицу, ответственному за обеспечение безопасности персональных данных, с просьбами об оказании необходимой нормативной и методической помощи в работе.

**5. Ответственность Ответственного лица**

Ответственное лицо несет дисциплинарную, административную уголовную ответственность в соответствии с действующим законодательством Российской Федерации и внутренними локальными актами ГАОУ ПО ИРО за:

5.1. Ненадлежащее выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией.

5.2. Правильность и объективность принимаемых решений.

5.3. Качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями.

5.4. Нарушение трудовой дисциплины, охраны труда, разглашение сведений ограниченного распространения, ставших известными ему в ходе выполнения должностных обязанностей.

5.5. В других случаях, предусмотренных законодательством Российской Федерации и внутренними локальными актами ГАОУ ПО ИРО.

Приложение № 3
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ПРАВИЛА

## доступа работников в помещения ГАОУ ПО «Институт развития образования», где осуществляется хранение и эксплуатация СКЗИ в рабочее и нерабочее время, а также в нештатных ситуациях

**г. Севастополь - 2024**

# ПРАВИЛА
## доступа работников в помещения ГАОУ ПО «Институт развития образования», где осуществляется хранение и эксплуатация СКЗИ в рабочее и нерабочее время, а также в нештатных ситуациях

### 1. Общие положения

1.1. Настоящие Правила устанавливают единые требования к доступу работников в помещения, где размещены и хранятся используемые СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ доступа работников в помещения, в рабочее и нерабочее время, а также в нештатных ситуациях (далее - Правила, Помещения).

1.2. Настоящие Правила разработаны в соответствии с нормативными правовыми актами Российской Федерации в области защиты персональных данных, требований к безопасной эксплуатации СКЗИ.

1.3. Правила обязательны для исполнения всеми работниками, которые участвуют в работе с СКЗИ, хранении СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

1.4. Нарушение Правил влечёт материальную, дисциплинарную, гражданскую, административную и (или) уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

1.5. В зданиях, где размещены и хранятся используемые СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, установлен пропускной режим (Приложение № 1).

1.6. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в них лиц, не имеющих права доступа.

1.7. Посетители (посторонние лица) пропускаются в ГАОУ ПО ИРО на основании паспорта. Охранник или дежурный заносит посещение в Журнал посещений, с указанием времени прибытия и убытия.

1.8. После 20-00 часов дежурный обязан произвести осмотр помещений ГАОУ ПО ИРО на предмет выявления посторонних лиц и оставленных подозрительных предметов.

1.9. Нахождение работников и посетителей в ГАОУ ПО ИРО после 18 час. 00 мин. без соответствующего разрешения руководителя запрещается.

### 2. Организация доступа в помещения

2.1. В Помещения допускаются только уполномоченные должностные лица и работники (Приложение № 2).

2.2. Нахождение в Помещениях, не указанных в пункте 2.1 лиц, возможно только в присутствии уполномоченного работника.

2.3. Уборка Помещений должна производиться в присутствии уполномоченного работника, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

При этом экраны мониторов должны быть выключены (либо осуществлена временная блокировка экранов/учетных записей пользователей автоматизированных рабочих мест), документы, находящиеся в печатающих устройствах, и учтенные носители информации должны быть убраны.

2.4. Доступ в Помещения разрешается только по рабочим дням в рабочее время (с 09 час. 00 до 18 час. 00 мин.).

2.5. Доступ в Помещения в нерабочее время возможен только по письменной заявке уполномоченного работника, согласованной с его непосредственным руководителем и имеющей разрешающую резолюцию руководителя ГАОУ ПО ИРО.

2.6. Первый пришедший на работу уполномоченный работник, рабочее место которого расположено в помещении, в котором осуществляется обработка персональных данных, получает на посту охраны ключ от этого помещения и расписывается в размещенном на посту охраны журнале с указанием времени получения ключа.

2.7. В случае, если в течение рабочего дня помещение, в котором осуществляется обработка персональных данных, покидают все уполномоченные работники, входная дверь этого помещения должна быть закрыта на ключ, который подлежит сдаче на пост охраны, и, в случае отсутствия в помещении датчика(ов) охранной сигнализации, опечатана специальным средством с внесением записи в журнал об опечатывании помещения.

2.8. Последний работник, покидающий (в том числе в течение рабочего дня и по его завершении) Помещение обязан:

- проверить закрытие на запоры окон и фрамуг;
- проверить отключение от электросети всех видов электрооборудования и электроприборов, не требующих по условиям эксплуатации постоянного подключения к электросети, отсутствие признаков загорания (запах гари, задымление и т.п.);
- выключить освещение в Помещении;
- закрыть Помещение на ключ, сдать ключ на пост охраны, при сдаче ключа от Помещения — одновременно расписаться в специальном журнале, находящемся на посту охраны (за сдачу ключей и произведенный осмотр Помещения) - с указанием времени сдачи;
- в случае отсутствия в Помещении датчика(ов) охранной сигнализации, опечатать специальным средством с внесением записи в журнал об опечатывании Помещения.

2.9. В случае возникновения нештатной ситуации (пожар, затопление, сбой в работе или выход из строя инженерных систем, совершение незаконных действий) работники коммунальных и аварийно-технических служб имеют право незамедлительного, беспрепятственного доступа в помещения, в которых ведется обработка персональных данных, в любое время суток, без какого-либо предварительного уведомления с целью предотвращения или ликвидации нештатной ситуации, или последствий нештатной ситуации.

2.10. По результатам предотвращения или ликвидации нештатной ситуации, или последствий нештатной ситуации оставляется акт вскрытия помещения при чрезвычайных ситуациях.

2.11. Ответственными за организацию доступа в Помещения являются руководители структурных подразделений, использующих Помещения.

Ответственный своевременно подготавливает/актуализирует и представляет на подпись руководителю ГАОУ ПО ИРО перечень лиц, имеющих право на получение на посту охраны и сдачу на пост охраны здания ключей от Помещений.

После подписания указанный в настоящем пункте перечень доводится до администрации/службы охраны.

**3. Ограничение доступа в помещения**

3.1. В целях соблюдения требований к ограничению доступа в Помещения обеспечивается:

- использованием Помещений строго по назначению;
- наличием на входах в Помещения дверей, оборудованных запорными устройствами;
- содержанием дверей и окон Помещений в нерабочее время в закрытом на запорное устройство состоянии.

Приложение № 1
к Правилам доступа в помещения

**ПЕРЕЧЕНЬ**
**мест размещения и хранения используемых СКЗИ и (или) носителей ключевой, аутентифицирующей и парольной информации СКЗИ**

| № п/п | Место размещения СКЗИ | Марка и учетный номер АРМ | Должность пользователя СКЗИ (лица имеющего право доступа) |
|---|---|---|---|
| 1 | Помещение «Приемная комиссия» г. Севастополь, ул. Советская д. 65 | АРМ «ICL» учетный (заводской) № 1013400363 | Начальник Центра информационно-программного обеспечения |
| | | | Начальник учебно-методического отдела |
| | | | Начальник сопровождения конкурсных процедур |
| | | | Инженеры-программисты |
| | | | Инженеры-электроники |
| | | | Специалисты по защите информации |
| | | | Другие должностные лица и работники в соответствии с приказами руководителя ГАОУ ПО ИРО |

Приложение № 2
к Правилам доступа в помещения

**ПЕРЕЧЕНЬ**
**уполномоченных должностных лиц и работников ГАОУ ПО «Институт развития образования», имеющих право доступа в помещения, где установлены и хранятся СКЗИ и ключевые документы к ним**

| № п/п | Место размещения средств криптографической защиты информации и ключевых документов | Должность уполномоченного лица |
|---|---|---|
| 1 | Помещение «Приемная комиссия» г. Севастополь, ул. Советская д. 65 | Директор |
| | | Заместитель директора по безопасности и ФЭД |
| | | Заместитель директора по учебно-методической работе |
| | | Начальник учебно-методического отдела |
| | | Начальник отдела сопровождения конкурсных процедур |
| | | Инженер-программист |
| | | Инженер-электроник |
| | | Специалисты по защите информации |
| | | Члены приемной комиссии, назначенные приказом руководителя ГАОУ ПО ИРО |

Приложение № 4
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ПРАВИЛА

## цель и способы обработки персональных данных в ФИС «ГИА и Приема»

**г. Севастополь - 2024**

# ПРАВИЛА, ЦЕЛЬ И СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФИС «ГИА И ПРИЕМА»

1. Цель обработки персональных данных в информационной системе персональных данных «Работа с ФИС «ГИА и Приема» - учет сведений об обучающихся и абитуриентах ГАОУ ПО ИРО.

2. Используемые способы обработки персональных данных: автоматизированная обработка, без передачи по внутренней сети ГАОУ ПО ИРО, с передачей по сети Интернет.

3. Перечень персональных данных, обрабатываемых в ФИС «ГИА и Приема»:

| **Субъект персональных данных** | **Категория персональных данных** | **Срок обработки персональных данных** |
|---|---|---|
| Обучающиеся | Фамилия, Имя, Отчество<br>Пол; Число, месяц, год рождения;<br>Сведения об образовании (наименование учебного заведения; год поступления; год окончания; наименование, регистрационный номер серия и номер документа об образовании, о квалификации по документу об образовании; о квалификации)<br>Уровень образования | -по достижении целей обработки;<br>- ограничивается сроком действия согласия субъекта персональных данных, предоставленного субъектом персональных данных |
| Выпускники | Фамилия, Имя, Отчество<br>Пол; Число, месяц, год рождения;<br>Сведения об образовании (наименование учебного заведения; год поступления; год окончания; наименование, регистрационный номер серия и номер документа об образовании, о квалификации по документу об образовании; о квалификации)<br>Сведения о подтверждении утраты документа об образовании;<br>Сведения о подтверждении обмена документа об образовании;<br>Страховой номер индивидуального лицевого счета | -по достижении целей обработки;<br>- ограничивается сроком действия согласия субъекта персональных данных, предоставленного субъектом персональных данных |
| Абитуриенты | Фамилия, Имя, Отчество<br>Пол; Число, месяц, год рождения;<br>Страховой номер индивидуального лицевого счета;<br>Сведения об образовании (наименование учебного заведения; год поступления; год окончания; наименование, регистрационный номер серия и номер документа об образовании, о квалификации по документу об образовании; о квалификации);<br>Сведения о подтверждении утраты документа об образовании;<br>Сведения о подтверждении обмена документа об образовании | -по достижении целей обработки;<br>- ограничивается сроком действия согласия субъекта персональных данных, предоставленного субъектом персональных данных |

4. Работа в ФИС «ГИА и Приема» осуществляется в помещении «Приемная комиссия», расположенном по адресу: г. Севастополь, ул. Советская д. 65.

5. Границами контролируемой зоны, в пределах которых размещены технические элементы ФИС «ГИА и Приема», определить ограждающие конструкции помещений расположенном по адресу: г. Севастополь, ул. Советская д. 65.

Приложение № 5
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

# ПЕРЕЧЕНЬ
## должностных лиц и работников ГАОУ ПО «Институт развития образования», имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ФИС «ГИА и Приема»

| № п/п | Место размещения | Должность уполномоченного лица |
|---|---|---|
| 1 | Помещение «Приемная комиссия» г. Севастополь, ул. Советская д. 65 | Директор |
| | | Заместитель директора по безопасности и ФЭД |
| | | Заместитель директора по учебно-методической работе |
| | | Начальник центра информационно-программного обеспечения |
| | | Начальник учебно-методического отдела |
| | | Начальник отдела сопровождения конкурсных процедур |
| | | Инженер-программист |
| | | Инженер-электроник |
| | | Специалисты по защите информации |
| | | Члены приемной комиссии, назначенные приказом руководителя ГАОУ ПО ИРО |
| | | Другие работники, назначенные приказом руководителя ГАОУ ПО ИРО |

Приложение № 6
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

# МАТРИЦА ДОСТУПА
## к защищаемым информационным ресурсам ФИС «ГИА и Приема»

1. Список субъектов доступа к защищаемым информационным ресурсам информационной системы персональных данных «Работа с ФИС «ГИА и Приема».

| № п/п | Роль | Учетная запись |
|---|---|---|
| 1 | Администратор | Admin* |
| 2 | Пользователь | User** |

*- При наличии нескольких администраторов добавляется дополнительный символ. (Например - Admin-1).

Администратор – назначаются отдельным приказом руководителя ГАОУ ПО ИРО.

**- При наличии нескольких пользователей добавляется дополнительный символ. (Например - User -1).

Пользователь, уровень доступа и перечень данных определяются отдельным приказом руководителя ГАОУ ПО ИРО по ходатайству руководителя структурного подразделения или лица ответственного за работу с персональными данными и иной конфиденциальной информации.

2. Список защищаемых ресурсов (объектов доступа) информационной системы персональных данных «Работа с ФИС «ГИА и Приема».

| № п/п | Наименование (тип) защищаемого ресурса | Место хранения защищаемого ресурса |
|---|---|---|
| 1 | Операционная система Microsoft Windows 10 Pro | %WINDIR% |
| 2 | Система защиты информации от несанкционированного доступа «DALLAS LOCK8.0-K» | %Program Files%\Dallas Lock80 |
| 3 | Программный комплекс «ViPNet Client 4» | %ProgramFiles%\InfOTeCS\ViPNet Client |
| 4 | Средство антивирусной защиты «Dr.WebEnterprise security Suite» | %ProgramFiles%\Dr. Web Enterprise \ Dr.WebEnterprise security Suite for Windows\ |
| 5 | Файлы, содержащие персональные данные | %USERPROFILE%Desktop %USERPROFILE %Documents |
| 6 | Федеральная информационная система «Федеральный реестр документов об образовании и (или) квалификации, документов об обучении» | http://10.3.47.15 |
| 7 | Федеральная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего | http://10.3.1:8080 |

Приложение № 7
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ПРАВИЛА

## осуществления в ГАОУ ПО «Институт развития образования» внутреннего контроля соответствия обработки персональных данных требованиям, предъявляемым к защите персональных данных

**г. Севастополь - 2024**

| | | |
|---|---|---|
| | профессионального и высшего образования и региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования | |
| 8 | Принтер | Вывод на печать |

3. Установленные права доступа субъектов доступа к защищаемым ресурсам информационной системы персональных данных «Работа с ФИС «ГИА и Приема»

| **Субъекты доступа** | **Наименование защищаемого ресурса, согласно списка защищаемых ресурсов (объектов доступа) информационной системы персональных данных «Работа с ФИС «ГИА и Приема»** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| Администратор | AERWD | AERWD | AERWD | AERWD | AERWD | AERWD | AERWD | AP |
| Пользователь | RE | RE | RE | RE | RE | RE | RE | P |

***Условные обозначения:*** **A** - администрирование; **E** - выполнение; **R** - чтение; **W** - запись; **D** - удаление; **P** - печать.

# ПРАВИЛА
## осуществления в ГАОУ ПО «Институт развития образования» внутреннего контроля соответствия обработки персональных данных требованиям, предъявляемым к защите персональных данных

### 1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 1 52-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и другими нормативными правовыми актами и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 1 52-ФЗ «О персональных данных».

### 2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. В целях осуществления внутреннего контроля в ГАОУ ПО ИРО должны проводиться периодические поверки условий обработки ПДн.

2.2. Проверка обработки ПДн в структурном подразделении учреждения проводится комиссией из числа работников ответственных за организацию обработки ПДн и представителей Центра информационно-программного обеспечения ГАОУ ПО ИРО, состав которой утверждается приказом руководителя ГАОУ ПО ИРО.

2.3. Плановые проверки условий обработки ПДн проводятся на основании утвержденного руководителем ГАОУ ПО ИРО плана мероприятий на календарный год.

2.4. Внеплановые проверки организации работы с ПДн проводятся на основании приказа руководителя ГАОУ ПО ИРО.

2.5. В проверке организации обработки ПДн не могут участвовать сотрудники ГАОУ ПО ИРО, прямо или косвенно заинтересованные в результатах проверки.

2.7. При проведении проверки условий обработки ПДн должны быть изучены вопросы:

- порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите ПДн;
- порядок и условия применения средств защиты информации;
- принимаемые меры по обеспечению безопасности ПДн до их ввода в информационные системы ПДн;
- состояние учета носителей ПДн;

•соблюдение правил доступа к ПДн;

•соблюдение порядка доступа в помещения, в которых ведется обработка ПДн;

•наличие (отсутствие) фактов несанкционированного доступа к ПДн;

•мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

•соответствие места хранения ПДн (материальных носителей) и соответствие перечня лиц, имеющих к ним доступ в установленном порядке;

•обеспечение раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях.

2.8. Права комиссии по проведению проверки условий обработки ПДн и вопросы, которые необходимо отразить при ее проведении определяются приказом руководителя ГАОУ ПО ИРО о проведении проверки.

2.9. Члены комиссии по проведению проверки должны обеспечить конфиденциальность ставшей им известной информации.

2.10. Проверка условий обработки ПДн должна быть завершена не позднее чем через 30 календарных дней со дня принятия решения об ее проведении.

2.11. По результатам проверки и мерах, необходимых для устранения выявленных нарушений, составляется акт, который представляется на утверждение руководителю ГАОУ ПО ИРО.

2.12. Назначение ответственных лиц, перечень мероприятий, необходимых для устранения и предотвращения нарушений в организации обработки ПДн, необходимость привлечения виновных должностных лиц к ответственности, установленной Законом и внутренними локальными документами ГАОУ ПО ИРО, осуществляется приказом руководителя ГАОУ ПО ИРО.

Приложение № 8
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

# ПЕРЕЧЕНЬ
## мест использования и хранения съёмных носителей персональных данных, информации ограниченного доступа и иной конфиденциальной информации

| № п/п | Структурное подразделение | Регистрационный номер СНКИ-ЭЦП | Владелец | Место хранения | Ответственный за хранение |
|---|---|---|---|---|---|
| 1 | Центр планирования и финансово-экономического обеспечения | ЭЦП-1 | Директор - физическое лицо | г. Севастополь, ул. Советская д. 65 | Начальник ЦПФЭО |
| | | ЭЦП-2 | Директор – юридическое лицо ГАОУ ПО ИРО | | |
| | | ЭЦП-3 | Директор – юридическое лицо ГАОУ ПО ИРО банк РНКБ | | |
| 2 | Центр кадрового учета, документооборота и канцелярии | ЭЦП-2 | Директор – юридическое лицо ГАОУ ПО ИРО | г. Севастополь, ул. Советская д. 65 | Начальник ЦПФЭО/Начальник ЦКУДК |
| 3 | Отдел по закупочной деятельности | ЭЦП-4 «Закупка» | Начальник отдела по закупочной деятельности | г. Севастополь, ул. Советская д. 65 | Начальник отдела |
| | | ЭЦП-5 «Закупки ГАОУ ПО ИРО» | Директор - юридическое лицо ГАОУ ПО ИРО | | |
| 4 | Отдел учебно-методической работы | ЭЦП-6 «ФИС ФРДО СПО/ПО» | Начальник отдела учебно-методической работы | г. Севастополь, ул. Терещенко д. 6 | Начальник отдела |
| 5 | Отдел сопровождения конкурсных процедур | ЭЦП-7 ФИС ФРДО ДПО» | Начальник отдела сопровождения конкурсных процедур | г. Севастополь, ул. Советская д. 54 | Начальник отдела сопровождения конкурсных процедур/Начальник ЦОПП |
| 6 | Центр опережающей профессиональной подготовки | | Начальник отдела сопровождения конкурсных процедур | | |

**Примечание:** Конкретное должностное лицо, ответственное за хранение СНКИ-ЭЦП, и место хранения назначаются приказом руководителя ГАОУ ПО ИРО.

Приложение № 9
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ИНСТРУКЦИЯ

## о порядке учета, хранения и использования съемных носителей ключевой информации в ГАОУ ПО «Институт развития образования»

**г. Севастополь - 2024**

# ИНСТРУКЦИЯ
## о порядке учета, хранения и использования съемных носителей ключевой информации

### 1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Приказом ФАПСИ от 13.06.2001 г. № 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» и другими нормативными актами, регулирующими использование съёмных носителей ключевой информации в организациях и учреждениях.

1.2. Настоящая Инструкция устанавливает порядок организации учета, хранения, выдачи и использования съемных носителей ключевой информации (далее СНКИ).

1.3. Действие Инструкция распространяется на съемные носители ключевой информации, эксплуатируемые в ГАОУ ПО ИРО и обязательно для исполнения всеми работниками ГАОУ ПО ИРО, имеющими и использующими СНКИ (далее - пользователи).

1.4. К съёмным носителям ключевой информации относятся и носители электронной цифровой подписи (СНКИ-ЭЦП): рутокены; флеш-носители и т.п.

### 2. Организация учета съемных носителей ключевой информации

2.1. Все виды носителей, находящиеся в обращении, подлежат учету в Журнале учета средств защиты информации.

2.2. Учет СНКИ осуществляют специалисты по защите информации. Факт выдачи СНКИ фиксируется в Журнале учета средств защиты информации.

2.3. Каждый СНКИ должен иметь уникальный номер, который присваивается специалистом по защите информации и наносится на бирку или на поверхность носителя.

### 3. Организация выдачи и использования СНК

3.1. Допускается использование только учтенных носителей информации, которые являются собственностью ГАОУ ПО ИРО и подвергаются регулярной ревизии, учёту и контролю технического состояния (работоспособности).

3.2. СНКИ предоставляются пользователям для шифрования (подписания) электронных документов, предназначенных для передачи по каналам связи.

3.3. Сотрудники ГАОУ ПО ИРО получают учтённый СНКИ для выполнения работ на конкретный срок от уполномоченного работника. При получении делаются соответствующие записи в Журнале учета средств защиты информации.

3.4. При использовании работниками СНКИ необходимо соблюдать следующие требования безопасности:

- не передавать СНКИ-ЭЦП третьим лицам;
- не сообщать никому пароль ключа электронной подписи;

•подключать СНКИ-ЭЦП к компьютеру только на время подписи документов или передачи документов в сторонние организации;

•помнить, что электронная подпись, находящаяся на ключевом носителе, равносильна личной подписи и печати на документах;

•исключить доступ посторонних лиц к компьютеру, на котором используется система шифрования/подписания/передачи информации сторонним организациям;

•своевременно устанавливать обновления операционной системы от производителя и регулярно обновлять антивирусные базы;

•не использовать на компьютере с установленной системой шифрования /подписания/передачи информации сторонним организациям средств удалённого доступа - удалённый рабочий стол, удалённый помощник и других;

•для настройки операционной системы и антивирусных программ привлекать специалистов Центра информационно-программного обеспечения ГАОУ ПО ИРО;

•не допускать воздействие на СНКИ: сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.), высоких и низких температур, магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;

•не прилагать излишних усилий при подключении СНКИ к компьютеру;

•в нерабочее время держать СНКИ закрытым во избежание попадания на разъем пыли, грязи, влаги и т.п.;

•при засорении разъема нужно принять меры для его очистки, используя сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо;

•не извлекать СНКИ во время процедуры записи и считывания.

3.5. В случае выявления фактов несанкционированного и/или нецелевого использования СНКИ проводится служебная проверка. Состав комиссии утверждается приказом руководителя ГАОУ ПО ИРО.

3.6. По результатам проверки составляется акт, который передается директору для утверждения и принятия мер в соответствии с действующим законодательством.

3.7. Информация, хранящаяся на СНКИ, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

3.8. Перед началом работы пользователь обязан проверить СНКИ на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютере.

3.9. В случае обнаружения вирусов - немедленно прекратить использование СНКИ и сообщить о данном факте специалисту по защите информации ГАОУ ПО ИРО.

3.10. Контроль выполнения работниками установленных правил эксплуатации СНКИ осуществляет руководитель структурного подразделения, отвечающего за хранение/учёт персональных данных, и специалисты по защите информации.

3.11. В случае увольнения, перевода работника в другое структурное подразделение или отстранения от работ, связанных с использованием СНКИ, предоставленные ему съемные носители ключевой информации изымаются. Факт изъятия фиксируется в Журнале учета средств защиты информации.

**4. Организация хранения съемных носителей информации**

4.1. Хранение СНКИ осуществляется в условиях, полностью исключающих несанкционированное копирование, изменение или уничтожение ключевой информации, а также хищение носителей.

4.2. СНКИ должны храниться в служебных помещениях в сейфе или в закрываемых шкафах, исключающих несанкционированный доступ к ним.

4.3. Запрещается хранить съемные носители ключевой информации вместе с носителями открытой информации, на рабочих столах, оставлять их без присмотра или передавать на хранение другим лицам.

**5. Действия при утрате или уничтожении съемных носителей информации**

5.1. В случае утраты или несанкционированного уничтожения СНКИ немедленно сообщить руководителю соответствующего структурного подразделения и специалисту по защите информации.

5.2. По факту утраты носителя составляется акт с внесением соответствующей информации в Журнал учета средств защиты информации.

**6. Ответственность при работе с съемными носителями информации**

6.1. Ответственность за выполнение правил эксплуатации СНКИ несет работник, эксплуатирующий СКЗИ.

6.2. В случае нарушения требования настоящей Инструкции, нарушитель несет ответственность в соответствии с действующим законодательством РФ и внутренними локальными актами ГАОУ ПО ИРО.

**7. Заключительные положения**

7.1. Настоящая Инструкция обязательна для выполнения всеми должностными лицами и работниками ГАОУ ПО ИРО.

Приложение № 10
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. .2024 г.

**ФОРМА ОБЯЗАТЕЛЬСТВА**
о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну

Я, *Фамилия, Имя, Отчество* исполняющий(ая) должностные обязанности по занимаемой должности: *Должность, наименование структурного подразделения* предупрежден(а), что на период исполнения должностных обязанностей, мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащим сведений, составляющих государственную тайну.

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В течение 3-х лет после прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

С положениями и инструкциями о порядке работы с персональными данными и иной конфиденциальной информацией ознакомлен(а).

_____ _____
(подпись) (Фамилия, инициалы)

«____» _____ 202___ г.

Приложение № 11
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ИНСТРУКЦИЯ

## ответственного за обеспечение безопасности персональных данных в ГАОУ ПО «Институт развития образования»

**г. Севастополь - 2024**

# ИНСТРУКЦИЯ
## ответственного за обеспечение безопасности персональных данных в ГАОУ ПО «Институт развития образования»

**1. Общие положения.**

1.1 Инструкция является локальным правовым актом, регламентирующим деятельность лица, ответственного за обеспечение безопасности персональных данных (далее - Ответственное лицо) в ГАОУ ПО «Институт развития образования» (далее – ГАОУ ПО ИРО) при выполнении функции по защите ПДн в ИСПДн.

1.2 Целью настоящей Инструкции является регламентирование работы лица, ответственного за обеспечение безопасности персональных данных в практической реализации мер защиты и обеспечения безопасности информации в используемых информационных системах персональных данных Оператора.

1.3 Назначение Ответственного лица, закрепление за ним определенных полномочий и обязанностей производится приказом руководителя ГАОУ ПО ИРО.

1.4 Ответственное лицо должно знать и применять в своей повседневной деятельности:

- законодательные акты, нормативные и методические материалы по вопросам, связанным с обеспечением защиты ПДн;
- структуру ИСПДн, особенности обработки ПДн в ней, перспективы её развития и модернизации;
- функции системы защиты персональных данных (далее СЗПДн);
- документацию на используемые в СЗПДн средства защиты информации;
- методы и средства контроля эффективности защиты ПДн, выявления каналов утечки информации;
- методы планирования и организации проведения работ по защите ПДн;
- технические средства контроля и защиты информации, перспективы и направления их совершенствования.

**2. Основные функции Ответственного лица.**

2.1 Обеспечение устойчивой работоспособности и безопасности ИСПДн в соответствии с нормативными правовыми актами, локальными актами по вопросам обработки и защиты персональных данных.

2.2 Организация работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в ИСПДн, а также правильность использования и штатного функционирования средств защиты информации, подготовку сотрудников (пользователей ИСПДн) по вопросам безопасной обработки информации в ИСПДн.

**3. Обязанности Ответственного лица**

3.1. Ответственный за обеспечение безопасности персональных данных должен организовывать выполнение следующих мероприятий по техническому обеспечению безопасности персональных данных при их обработке в ИСПДн:

- по предоставлению и разграничению доступа в информационные системы персональных данных;

•по закрытию технических каналов утечки персональных данных, при их наличии;

•по защите от несанкционированного доступа к персональным данным;

•по выбору средств защиты персональных данных;

•по своевременному обнаружение фактов несанкционированного доступа к персональным данным, обрабатываемым в ИСПДн;

•по недопущению воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование;

•по обеспечению возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

•по обеспечению хранения двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности;

•по постоянному контроль за обеспечением уровня защищенности персональных данных, при их обработке в ИСПДн;

•по проведению внутренних проверок состояния технической защиты персональных данных не менее двух раз в год;

•по определению событий безопасности, подлежащих регистрации, и сроков их хранения, а так же состава и содержания информации о событиях безопасности, подлежащих регистрации;

•по определению лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;

•по осуществление контроля за соблюдением условий использования средств защиты информации (в том числе криптографических), предусмотренных эксплуатационной и технической документацией;

•по организации периодической проверки электронных журналов автоматизированных средств ИСПДн с целью анализа запросов пользователей ИСПДн на получение доступа к персональным данным, а также актов предоставления персональных данных по этим запросам;

•по организации периодической проверки электронных журналов средств защиты информации с целью анализа событий, представляющих опасность для защищаемых персональных данных;

•по организации ведения поэкземплярного учета носителей персональных данных, применяемых средств защиты (в том числе криптографических), а также эксплуатационной и технической документации к ним;

•по подготовке отчетов о состоянии работ по обеспечения технической защиты персональных данных;

•по осуществлению текущего и периодического контроля работоспособности средств и систем защиты ПДн;

•по осуществлению периодического контроля за действиями сотрудников при работе с паролями, соблюдением правил их хранения и использования;

•по осуществлению планирования и проведения мероприятий по антивирусной защите;

•по обеспечению формирования и поддержания в актуальном состоянии матрицы доступа сотрудников к защищаемым ресурсам ИСПДн;

•по осуществлению автоматизированного контроля текущего функционального состояния ИСПДн, включающего просмотр журнала активных сеансов, контроль за работой конкретного рабочего места;

•по поддержанию непрерывного функционирования системы защиты персональных данных;

•по проведению ознакомления пользователей ИСПДн с правилами работы со средствами защиты информации.

3.2. Ответственный за обеспечение безопасности персональных данных обязан:

3.2.1. Участвовать в подготовке объектов Оператора к аттестации по выполнению требований обеспечения безопасности персональных данных, в случае принятия руководством Оператора решения о необходимости проведения аттестации.

3.2.2. Участвовать в проводимых работах по совершенствованию системы защиты персональных данных.

3.2.3. Участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой ПДн, попыток несанкционированного доступа в ИСПДн, несоблюдения правил и условий работы в ИСПДн, хранения носителей персональных данных, использования средств защиты информации (в том числе криптографических) и иных нарушений, снижающих уровень защищенности персональных данных, разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений;

3.2.4. Информировать руководителя ГАОУ ПО ИРО о фактах нарушения установленного порядка работ, попытках несанкционированного доступа к информационным ресурсам ИСПДн, действиях сотрудников, нарушающих установленные требования к обеспечению безопасности персональных данных.

**4. Права Ответственного лица.**

4.1. Ответственный за обеспечение безопасности персональных данных имеет право:

•требовать от должностных лиц, допущенных к обработке персональных данных, безусловного соблюдения установленных правил обработки и защиты персональных данных;

•вносить свои предложения по совершенствованию мер защиты персональных данных;

•ходатайствовать перед руководителем ГАОУ ПО ИРО о прекращении обработки информации, как в целом в ИСПДн, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн;

•обращаться к руководителю ШАОУ ПО ИРО с просьбами об оказании необходимой нормативной и методической помощи в работе;

•получать доступ во все помещения, в которых осуществляется обработка персональных данных;

**4. Ответственность Ответственного лица.**

4.1. Ответственное лицо несет дисциплинарную, административную, уголовную ответственность, в соответствии с законодательством Российской Федерации в области защиты персональных данных и внутренними локальными правовыми актами ГАОУ ПО ИРО за:

- невыполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;
- правильность и объективность принимаемых решений;
- некачественное проведение работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;
- несоблюдение трудовой дисциплины, охраны труда, разглашение сведений ограниченного распространения, ставших известными ему в ходе выполнения должностных обязанностей;
- в других случаях, предусмотренных законодательством Российской Федерации в области защиты персональных данных и внутренними локальными правовыми актами ГАОУ ПО ИРО.

Приложение № 12
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ИНСТРУКЦИЯ

## о порядке технического обслуживания, ремонта, модернизации технических и программных средств, средств защиты информации, входящих в состав информационных систем обработки персональных данных ГАОУ ПО «Институт развития образования»

**г. Севастополь - 2024**

# ИНСТРУКЦИЯ

**о порядке технического обслуживания, ремонта, модернизации технических и программных средств, средств защиты информации, входящих в состав информационных систем обработки персональных данных ГАОУ ПО «Институт развития образования»**

**1. Общие положения.**

1.1. Данная инструкция регламентирует порядок взаимодействия структурных подразделений ГАОУ ПО «Институт развития образования» по вопросам обеспечения безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники, используемой при обработке персональных данных и при возникновении нештатных ситуаций в работе АС.

1.2. Перечень использованных сокращений, единиц и терминов

| | | |
|---|---|---|
| АС | – | автоматизированная система |
| АСО | – | активное сетевое оборудование |
| АРМ | – | автоматизированное рабочее место |
| АЭД | – | архив эталонных дистрибутивов |
| ИБ | – | информационная безопасность |
| ИС | – | информационная система |
| ИТ (IT) | – | информационные технологии |
| КИС | – | корпоративная информационная система |
| ЛВС | – | локальная вычислительная сеть |
| НСД | – | несанкционированный доступ |
| АИБ | – | администратор информационной безопасности |
| ПК | – | персональный компьютер |
| ПО | – | программное обеспечение |
| ПЭВМ | – | персональная электронная вычислительная машина |
| СБ | – | служба безопасности |
| СЗИ | – | средства защиты информации |
| СУБД | – | система управления базами данных |
| ФСТЭК | – | Федеральная служба по техническому и экспортному контролю |
| ЭД | – | эксплуатационная документация |

1.3. Администратор информационной безопасности - специалист по защите информации, осуществляющий мероприятия по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации, обеспечивающий защиту конфиденциальной информации и персональных данных.

**2. Права и обязанности структурных подразделений ГАОУ ПО ИРО по внесению изменений в конфигурацию технических и программных средств.**

2.1. Все изменения должны производиться только на основании заявок руководителей структурных подразделений, согласованных с администратором информационной безопасности.

2.2. Внесение изменений в конфигурацию аппаратно-программных средств

(материнская плата, жесткий диск, дисковод, CD-ROM, DVD-ROM, СЗИ (аппаратные, аппаратно-программные, программные), ПО) рабочих станций и серверов в отношении: системных и прикладных программных средств; программно-аппаратных средств защиты информации и персональных данных; программно-аппаратных средств телекоммуникации производится администратором информационной безопасности (при необходимости, с привлечением инженера-электроника или других специалистов).

2.3. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме администратора информационной безопасности, **запрещено**.

**3. Порядок оформления заявок.**

3.1. Процедура внесения изменений в конфигурацию аппаратных и программных средств серверов и рабочих станций инициируется заявкой руководителя структурного подразделения ГАОУ ПО ИРО, либо администратором информационной безопасности по установленной форме (Приложении №1).

3.2. Заявка руководителя структурного подразделения, в которой требуется произвести изменения конфигурации АРМ, оформляется администратором информационной безопасности.

3.3. Руководитель структурного подразделения, использующего АРМ, требующую модификации, информируется перед проведением работ (не позднее чем за 1 день до начала работ).

3.4. Перечень изменения в составе аппаратных и программных средств АРМ и серверов:

- установка в подразделении новой ПЭВМ (развертывание нового АРМ или сервера);
- замена ПЭВМ (АРМ или сервера подразделения);
- изъятие ПЭВМ (АРМ или сервера подразделения);
- добавление устройства (узла, блока) в состав конкретного АРМ или сервера подразделения;
- замена устройства (узла, блока) в составе конкретного АРМ или сервера подразделения;
- изъятие устройства (узла, блока) из состава конкретного АРМ или сервера;
- обновление (восстановление) системного ПО;
- установка (развертывание) на конкретное АРМ или сервера программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данном АРМ или сервере), за исключением офисного ПО.

3.5. В заявке указываются условные наименования развернутых АРМ и серверов в соответствии с их формулярами (регистрационными карточками).

3.6. В случае развертывания нового АРМ его наименование в заявке указывать не требуется (оно устанавливается позднее при заполнении формуляра нового АРМ).

3.7. Наименования задач указываются в соответствии с формулярами задач или перечнем задач архива эталонных дистрибутивов, которые можно решать с использованием АС.

3.8. Заключение о технической возможности осуществления затребованных изменений и непосредственного исполнения работ по внесению изменений в конфигурацию АРМ или серверов АС проводится администратором информационной

хранилась на дисках компьютера.

4.7. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора информационной безопасности.

4.8. В случае поломки жесткого диска в договоре, при передаче его в организацию для осуществления ремонта, должна быть предусмотрена ответственность сторонней организации о неразглашении информации, содержащейся на передаваемом диске.

4.9. Допуск новых пользователей к решению задач с использованием вновь установленного ПО (либо изменение их полномочий доступа) осуществляется согласно установленным правилам предоставления доступа к информационному ресурсу.

4.10. Оригиналы документов, на основании которых производились изменения в составе технических или программных средств АРМ с отметками о внесении изменений в состав аппаратно-программных средств, должны храниться у администратора информационной безопасности.

Они могут использоваться в следующих случаях:

- для восстановления конфигурации АРМ после аварий;
- для контроля правомерности установки на конкретной АРМ средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты АРМ.

4.11. Регулярные. внеплановые проверки исправности и техническое обслуживание технических средств, средств защиты информации и персональных данных отражаются в журнале проверки исправности и технического обслуживания.

**5. Экстренная модификация (обстоятельства форс-мажор).**

5.1. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на рабочей станции.

В данной ситуации администратор информационной безопасности в известность своего руководителя о необходимости такого изменения.

5.2. Факт внесения изменений в ПО АРМ оформляется актом за подписями администратором информационной безопасности и пользователя данного АРМ.

В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), осуществившее изменения.

При необходимости проводится изменение ПО загрузочного раздела сервера. Если это необходимо, администратор информационной безопасности вносит необходимые корректировки в настройки системы контроля целостности ПО АРМ и сервера (при их использовании).

5.3. Факт модификации ПО и корректировок настроек системы защиты фиксируется на АРМ (сервере).

5.4. В течение следующего дня после составления акта, администратор информационной безопасности выясняет причины и состав проведенных экстренных изменений и принимают решение о необходимости подготовки исправительной модификации ПО или восстановления ПО АРМ (сервера) с эталонной копии (из АЭД).

Результат проверки оформляется в виде согласованного решения и хранится у администратора информационной безопасности.

безопасности.

**4. Порядок производства работ.**

4.1. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится администратором информационной безопасности.

*Если АРМ или сервер относится к защищаемым рабочим станциям, то установка и внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов (при их использовании) на АРМ осуществляется администратором информационной безопасности.*

*В случае необходимости работы производятся в присутствии пользователя данной АРМ.*

4.2. Подготовка модификаций программного обеспечения защищенных серверов и АРМ, тестирование, стендовые испытания и другие необходимые действия производятся администратором информационной безопасности.

*Установка или обновление подсистем АС должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.*

4.3. Модификация ПО серверов осуществляется администратором информационной безопасности.

*При использовании СЗИ, после установки модифицированных модулей на сервер администратор информационной безопасности устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью средств СЗИ).*

4.4. Установка и обновление общего ПО (системного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), а прикладного ПО - с эталонных копий программных средств (при реализации сетевого архива эталонных дистрибутивов программ – из него).

*При необходимости (в случае установки части компонент на дисках сетевых серверов) к работам привлекается администратор информационной безопасности.*

*Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность.*

4.5. После установки (обновления) ПО администратор информационной безопасности должен произвести настройку СЗИ от НСД в соответствии с ее (его) формуляром.

*Настройка должна осуществляться совместно с ответственным пользователем АРМ.*

*Администратор информационной безопасности должен проверить работоспособность ПО и правильность настройки средств защиты.*

*После завершения работ по внесению изменений в состав аппаратных средств защищаемого АРМ и его системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) администратором информационной безопасности.*

4.6. Изъятие АРМ из состава рабочих станций подразделения при ее передаче на склад, в ремонт или в другое подразделение осуществляется только после того, как администратор информационной безопасности снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для удаления защищаемой информации, которая

**6. Порядок технического обслуживания и ремонта технических средств АРМ (серверов) АС.**

6.1. Самостоятельное техническое обслуживание и ремонтные работы на технических средствах ПЭВМ АРМ должны осуществляться только администратором информационной безопасности.

Вызов администратора информационной безопасности осуществляется сотрудниками подразделения, эксплуатирующих АРМ, при возникновении нештатных ситуаций.

6.2. К нештатным ситуациям относятся:

- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (например, дисковода, принтера) АРМ;
- выход из строя системы электроснабжения АРМ.

6.3. Техническое обслуживание и регламентные работы могут проводиться в плановом порядке.

6.4. Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на ПЭВМ возлагается на администратора информационной безопасности.

6.5. При необходимости осуществления изменений аппаратно-программной конфигурации АРМ соответствующие работы выполняются с соблюдением требований данной Инструкции.

**7. Порядок проверки работоспособности системы защиты после установки (обновления) программных средств и внесения изменений в списки пользователей.**

7.1. После установки (обновления) программных средств АРМ или внесения изменений в списки пользователей системы администратор информационной безопасности обязан проверить работоспособность АРМ и правильность настройки средств защиты, установленных на компьютере в соответствии с инструкциями на конкретные СЗИ.

7.2. После осуществления данных действий необходимо проверить корректность функционирования системы защиты.

Начальнику Центра информационного-
программного обеспечения ГАОУ ПО ИРО

**ЗАЯВКА**
**на внесение изменений в состав аппаратно-программных средств ИС**

Прошу поручить подчиненным Вам специалистам по защите информации произвести следующие изменения конфигурации аппаратно-программных средств ПЭВМ *Наименование структурного подразделения* (развернуть новую рабочую станцию и установить на (обновить на/снять с) нее _____ компоненты), необходимые для решения следующих задач:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Руководитель структурного подразделения СОГЛАСОВАНО _____ (подпись) _____ (фамилия и инициалы)

Заместитель директора по безопасности и финансово-экономической деятельности _____ (подпись) _____ (фамилия и инициалы)

«___» _____ 202__ г.

**Отметка о выполнении**
**(о внесении изменений в состав аппаратно-программных средств ИС)**

В соответствии с «Инструкцией о порядке технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав автоматизированной системы, обрабатывающей персональные данные» ***Наименование системы*** рабочей группой в составе:

Администратор информационной безопасности:

_____

от подразделения (отдела) _____

указанные в заявке изменения внесены (не внесены по следующей причине).

_____
краткое пояснение причины

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Изменения в формуляр АРМ (ссылка на данную заявку) внесены.

От подразделения

_____

_____
(подпись, фамилия)

«___» _____ 202__ года

Администратор информационной безопасности

_____
(подпись, фамилия)

«___» _____ 202__ года

УТВЕРЖДАЮ
Руководитель ГАОУ ПО ИРО
(лицо уполномоченное, согласно приказа руководителя)
_____ _____

«___» _____ 202__ г.

**АКТ**
**об удалении информации, хранившейся на диске компьютера**

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД №_____, передаваемого _____
(с какой целью)

_____
(Кому: должность, Ф.И.О.)

системного блока ПЭВМ марки _____ серийный №_____
уничтожены (затерты) посредством программы _____

Администратор информационной безопасности

_____
(Ф.И.О.)

_____ _____
(Подпись) (Дата)

Приложение № 13
к приказу ГАОУ ПО ИРО
№ 819 от 05.11. 2024 г.

Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»

# ПОЛОЖЕНИЕ

## по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации ГАОУ ПО «Институт развития образования»

**г. Севастополь - 2024**

# ПОЛОЖЕНИЕ
## по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации ГАОУ ПО «Институт развития образования»

### 1. Общие положения

1.1. Настоящее Положение по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации ГАОУ ПО «Институт развития образования» (далее -ГАОУ ПО ИРО; Положение) разработано в соответствии с:

- Федеральным законом РФ от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федерального агентства правительственной связи и информации при Президенте РФ от 13.06.2001 г. № 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»;
- Приказом Федеральной службы безопасности РФ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказом ФСБ России от 10.07.2014 г. № 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»;
- Методическими рекомендациями 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 (утверждены руководством 8 Центра ФСБ России 31.03.2015 г. № 149/7/2/9-432).

1.2. К шифровальным (криптографическим) средствам защиты информации (далее -СКЗИ), включая документацию на эти средства, относятся:

- *Средства шифрования* - аппаратные, программные и программноаппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;
- *Средства имитозащиты* - аппаратные, программные и программноаппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания

ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации; средства электронной подписи;

•*Средства кодирования* - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций; средства для изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящих в состав этих шифровальных (криптографических) средств;

•*Ключевые документы* - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.

**2. Организация и обеспечение функционирования СКЗИ**

2.1. Организация и обеспечение функционирования СКЗИ представляет следующий комплекс мероприятий:

•установка и ввод в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам;

•проверка готовности СКЗИ к использованию с составлением заключений о возможности их эксплуатации;

•разработка мероприятий по обеспечению 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;

•создание исходной ключевой информации, создание из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;

•обучение сотрудников, использующих СКЗИ, работе с ними;

•поэкземплярный учет используемых СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;

•проведение служебной проверки и составление заключений по фактам нарушения условий криптографической защиты информации.

**3. Структура ответственных лиц**

3.1. Структуру ответственных лиц по направлению организации и обеспечению криптографической защиты информации образуют:

•ответственный пользователь СКЗИ;

•пользователи СКЗИ.

3.2. Лица, осуществляющие работу с СКЗИ, должны быть ознакомлены с документами, регламентирующими организацию и обеспечение криптографической защитой информации, под подпись и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством РФ.

3.3. Контроль за организацией и обеспечением функционирования СКЗИ возлагается на ответственного пользователя СКЗИ в пределах его служебных полномочий.

3.4. Контроль за организацией, обеспечением функционирования и безопасности СКЗИ осуществляется в соответствии с законодательством РФ.

**4. Ответственный пользователь СКЗИ**

4.1. Ответственный пользователь СКЗИ назначается приказом руководителя ГАОУ ПО ИРО.

4.2. На ответственного пользователя СКЗИ возлагаются функции: органа криптографической защиты, организации и обеспечения функционирования СКЗИ.

4.3. Перед допуском к работе ответственный пользователь СКЗИ обязан ознакомиться с нормативными правовыми документами, регулирующими организацию и обеспечение криптографической защиты информации, настоящим Положением и локальными актами, определяющими порядок защиты информации с помощью СКЗИ.

4.4. Ответственный пользователь СКЗИ осуществляет:

- организацию безопасности обработки информации с использованием СКЗИ;
- обеспечение функционирования и безопасности СКЗИ;
- организацию и обеспечение эксплуатации СКЗИ;
- разработку и осуществление мероприятий по организации и обеспечению безопасности хранения, обработке и передаче информации с использованием СКЗИ;
- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей, ключевых документов;
- учет сотрудников, являющихся пользователями СКЗИ;
- заводит и ведет на каждого пользователя СКЗИ лицевой счет, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;
- обучение пользователей СКЗИ работе с СКЗИ;
- инсталляцию (деинсталляцию) СКЗИ с рабочих мест пользователей СКЗИ, прием, выдачу, уничтожение ключевой информации, эксплуатационной и технической документации к ним;
- плановую смену ключей, а также смену ключей в случае их компрометации;
- контроль за соблюдением пользователями СКЗИ условий использования СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- участие в комиссиях по расследованию фактов нарушений условий использования СКЗИ, которые могут привести (привели) к снижению уровня характеристик безопасности информации;
- участие в комиссиях по плановой проверке правильности учета и соблюдения правил обращения с СКЗИ и их хранением;
- уведомление руководства о фактах нарушения порядка эксплуатации СКЗИ.

4.5. Ответственный пользователь СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности хранения, обработки с использованием СКЗИ требованиям законодательства, эксплуатационной и технической документации к СКЗИ, настоящим Положением

**5. Пользователь СКЗИ**

5.1 Пользователь СКЗИ обязан:

- не разглашать информацию, к которой он допущен, в том числе сведения об СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- обеспечивать с помощью СКЗИ безопасность хранения, обработки информации, ключевых документов к СКЗИ и парольной информации к ним;
- осуществлять эксплуатацию СКЗИ в соответствии с требованиями эксплуатационной документации;
- не допускать снятие копий с ключевых документов;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевых документов на объекты информатизации (далее - ОИ);
- хранить 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;
- предусматривать раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей;
- сообщать о ставших известных попытках получения сведений об используемых СКЗИ или ключевых документах к ним лицами, не обладающими правом доступа к таким сведениям;
- немедленно уведомлять ответственного пользователя СКЗИ, руководство о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее — Помещения), хранилищ, личных печатей, предназначенных для опечатывания Помещений (хранилищ), и о других фактах, которые могут привести к снижению уровня характеристик безопасности информации;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

**6. Требования к обеспечению безопасности хранения и обработки информации с использованием СКЗИ**

6.1. Безопасность хранения и обработки с использованием СКЗИ информации достигается:

- соблюдением пользователями СКЗИ конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;
- точным выполнением пользователями СКЗИ требований к обеспечению безопасности информации;
- надежным хранением эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации;

•своевременным выявлением сотрудниками попыток получения сведений о защищаемой информации, об используемых СКЗИ или ключевых документах к ним лицами, не обладающими правом доступа к таким сведениям;

•немедленным принятием мер по предупреждению разглашения защищаемой информации, а также возможной ее утечки при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от Помещений, хранилищ, сейфов, личных печатей и т.п.

**7. Требования к помещениям**

7.1. Размещение, специальное оборудование, охрана и организация режима в Помещениях, должны обеспечивать сохранность защищаемой информации, СКЗИ и ключевых документов к ним.

7.2. Помещения должны удовлетворять требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

7.3. Размещение, специальное оборудование, охрана и организация режима в Помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.4. Обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих права доступа в Помещения, который достигается путем:

•оснащением Помещений входными дверьми с замками;

•обеспечением постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

•утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

•утверждения перечня лиц, имеющих право доступа в Помещения. Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.

7.5. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие Помещений в нерабочее время.

7.6. Для предотвращения просмотра Помещений извне их окна должны быть защищены.

7.7. Ответственный пользователь СКЗИ осуществляет учет хранилищ, ключей от них в журнале учета хранилищ и ключей от них.

7.8. Помещения подлежат опечатыванию или должны быть оснащены охранной сигнализацией, связанной со службой охраны здания.

7.9. Исправность охранной сигнализации периодически необходимо проверять с отметкой в журнале проверки работы средств охранной сигнализации, размещенных в помещении.

7.10. Ключи от дверей Помещений подлежат учету, который осуществляет ответственный пользователь СКЗИ в журнале учета хранилищ и ключей от них.

7.11. Личные печати сотрудников, предназначенные для опечатывания хранилищ и Помещений, должны находиться у пользователей СКЗИ, ответственных за эти хранилища и Помещения.

7.12. Выдачу личных печатей сотрудникам осуществляет ответственный пользователь СКЗИ с отметкой в журнале учета личных печатей, предназначенных для опечатывания помещений (хранилищ).

7.13. По окончании рабочего дня Помещения и установленные в нем хранилища должны быть закрыты, а также поставлены на охрану посредством технических средств охраны или опечатаны.

7.14. При утрате ключа от хранилища или от входной двери в Помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

7.15. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в Помещения о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ или руководству.

Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации и к замене скомпрометированных криптоключей.

7.16. Обеспечение сохранности носителей персональных данных достигается:

- хранением 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. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);
- поэкземплярный учетом машинных носителей персональных данных в соответствующем журнале.

7.17. В Помещениях для хранения выданных им ключевых документов, эксплуатационной и технической документации к СКЗИ, инсталлирующих СКЗИ носителей необходимо наличие достаточного числа надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин.

Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

**8. Требования к СКЗИ**

8.1. Для криптографической защиты информации должны применяться только сертифицированные по требованиям Федеральной службы безопасности РФ СКЗИ.

8.2. Требования к объектам информатизации, на которые инсталлируются СКЗИ, технические характеристики и состав ПО должны соответствовать требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ.

8.3. 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).

8.4. Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

8.5. При наличии технической возможности на время отсутствия пользователей СКЗИ данные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

**9. Требования к криптоключам**

9.1. По истечению срока действия, криптоключ подлежит смене, в порядке, предусмотренном эксплуатационной и технической документацией к СКЗИ или регламентом удостоверяющего центра, от которого получен ключевой документ.

**10. Эксплуатация СКЗИ**.

10.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним.

10.2. Единицей поэкземплярного учета криптоключей является ключевой носитель.

10.3. Если один и тот же ключевой носитель многократно используется для записи криптоключей, то каждый раз он подлежит отдельной регистрации. Журналы ведутся ответственным пользователем СКЗИ.

10.4. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале или в журнале поэкземплярного учета ключевых носителей, ключевых документов, ведущимся непосредственно пользователем СКЗИ.

10.5. Выдача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов осуществляется ответственным пользователем СКЗИ под подпись в соответствующем журнале учета.

10.6. Перед инсталляцией СКЗИ проводится обследование Помещения на соответствие требованиям, предъявляемым к Помещениям технической и эксплуатационной документацией к СКЗИ.

**11. Порядок эксплуатации СКЗИ.**

11.1. Эксплуатация СКЗИ осуществляется в соответствии с технической и эксплуатационной документацией к нему.

11.2. Эксплуатационная и техническая документация для СКЗИ, ключевые документы хранятся в хранилищах в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

11.3. Отдельно от ключей подлежат хранению резервные ключевые документы, предназначенные для применения в случае компрометации действующих.

11.4. Перед началом работы с ОИ контролируется наличие и целостность номерной наклейки (пломбы), которой опечатан системный блок.

11.5. После входа в операционную систему контролируется запуск антивирусного программного обеспечения и актуальность антивирусных баз.

11.6. Во время эксплуатации СКЗИ осуществляется контроль целостности установленного СКЗИ с помощью механизма самого СКЗИ или с помощью программного обеспечения контроля целостности.

11.7. Во время эксплуатации СКЗИ пользователям СКЗИ запрещается:

- изменять настройки СКЗИ;

•осуществлять вскрытие системного блока ОИ с установленными СКЗИ, подключать к ним дополнительные устройства без разрешения ответственного пользователя СКЗИ;

•оставлять без контроля ключевые носители, а также ОИ с установленными СКЗИ при включенном питании;

•вносить какие-либо несанкционированные изменения в СКЗИ;

•выводить на монитор защищаемую информацию (в т.ч. информацию ключевых документов), обрабатываемых с использованием СКЗИ в присутствии лиц, не имеющих к такой информации права доступа;

•применять скомпрометированные ключи и пароли;

•осуществлять несанкционированное копирование ключевой информации;

•вставлять ключевой носитель в устройства, штатный порядок работы которых не предусматривает использование ключевого носителя.

**12. Контроль за соблюдением эксплуатации средств криптографической защиты информации**

12.1. Контроль за соблюдением эксплуатации средств криптографической защиты информации проводится ежегодно – комиссией, назначаемая приказом руководителя ГАОУ ПО ИРО, которая:

•проверяет наличие, правильность учета и соблюдения правил обращения и хранения СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

•определяете установочные носители СКЗИ, ключевые документы, экземпляры технической и эксплуатационной документации, подлежащие уничтожению;

•проверяет соблюдение правил обращения, предусмотренных настоящим Положением пользователями СКЗИ.

12.2. Внеплановые проверки проводятся комиссией, назначенной приказом руководителя ГАОУ ПО ИРО, в случаях нарушения установленного порядка криптографической защиты информации.

12.3. По завершении проверки комиссией составляется Акт проверки, в котором указывается состав комиссии, основание проверки, проверочные мероприятия, недостатки, выявленные в ходе проверки, и рекомендации по их устранению, рекомендации по совершенствованию криптографической системы защиты информации.

**13. Порядок проведения служебной проверки по фактам нарушения правил эксплуатации СКЗИ**

13.1. В случае возникновения конфликтной ситуации и по фактам (подозрению) нарушения конфиденциальности информации, защищаемой с помощью СКЗИ, проводится служебная проверка.

13.2. Основаниями проведения служебной проверки являются информационные письма (претензии) сторонних организаций, непосредственное обнаружение факта (подозрения) нарушения конфиденциальности защищаемой информации, безопасность которых обеспечивается применением СКЗИ.

13.3. Служебная проверка назначается руководителем не позднее трех дней с момента поступления информации о факте нарушения конфиденциальности защищаемой информации.

13.4. В ходе служебной проверки устанавливается:

- действительно ли имело место нарушение конфиденциальности защищаемой информации;
- лица виновные в нарушении, их вина и ее степень;
- причины и условия, способствовавшие нарушению;
- характер и размер причиненного ущерба;
- предложения по недопущению подобных случаев впредь;
- иные сведения, имеющие отношения к нарушению.

13.5. Служебная проверка осуществляется комиссией, состав комиссии утверждается руководителем ГАОУ ПО ИРО, состав комиссии должен представлять не менее трех человек.

13.6. Срок завершения служебной проверки указывается в документе о проведении служебной проверки. Если срок не указан, то служебная проверка завершается не позднее, чем через месяц со дня обнаружения нарушения.

13.7. Результаты проверки оформляются Заключением, в котором указываются основание и сроки проведения служебной проверки, состав комиссии, значимые обстоятельства, установленные в ходе служебной проверки. Акт подписывается всеми членами комиссии и направляется руководителю.

**14. Порядок действий при компрометации ключа**

14.1. Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

14.2. Различают явную и неявную компрометацию ключей.

14.2.1. Явная компрометация - факт который становится известным на отрезке установленного времени действия данного ключа.

События, квалифицируемые как явная компрометация:

- утрата ключевого носителя;
- утрата ключевого носителя с последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации.

14.2.2.Неявная компрометация ключа - факт который остается неизвестным для лиц, являющихся законными пользователями данного ключа.

К событиям, связанным с неявной компрометацией ключей и требующим их рассмотрения в каждом конкретном случае, относятся:

- навязывание заведомо ложной информации в документах, защищенных имитовставками;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями, содержащими ключевую информацию, в том числе случаи, когда дискета (eToken и др.) вышла из строя и доказательно не опровергнуто, что данный факт произошел в результате несанкционированного доступа злоумышленника.

14.3. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их чтения, копирования.

14.4. При наступлении компрометации ключа или подозрения в компрометации ключа пользователь СКЗИ обязан немедленно прекратить работу с СКЗИ и сообщить ответственному пользователю СКЗИ о факте компрометации (в том числе и предполагаемом).

14.5. По факту компрометации ключей (в том числе предполагаемому) проводится служебная проверка в соответствии с п. 13 настоящего Положения.

14.6. По завершению проверки оформляется письменное заключение (акт) о проведении служебной проверки.

14.7. По завершению проверки, скомпрометированные ключи подлежат уничтожению в порядке, определенном настоящим Положением.

14.8. Взамен скомпрометированных ключей ответственный пользователь СКЗИ производит замену ключей в порядке, предусмотренном технической и эксплуатационной документацией, или в соответствии с Регламентом удостоверяющего центра

**15. Деинсталляция средств криптографической защиты информации**

15.1. Деинсталляция СКЗИ с рабочих мест пользователей СКЗИ осуществляется на основании решения руководителя или по соответствующей заявке.

15.2. Деинсталляция СКЗИ осуществляется комиссией в соответствии с процедурой, предусмотренной эксплуатационной и технической документацией к СКЗИ, с составлением Акта деинсталляции СКЗИ.

15.3. Акт о деинсталляции СКЗИ подлежит хранению у ответственного пользователя СКЗИ.

15.4. В состав комиссии включается ответственный пользователь СКЗИ.

15.5. Одновременно с деинсталляцией СКЗИ уничтожаются криптоключи, если не планируется их дальнейшее использование. В противном случае они возвращаются ответственному пользователю СКЗИ с отметкой в соответствующем журнале.

15.6. О факте деинсталляции СКЗИ делается отметка в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

**16. Уничтожение СКЗИ**

16.1. Основаниями для уничтожения инсталляционных носителей СКЗИ, эксплуатационной и технической документации к ним, ключевых документов являются утвержденные акты на списание и уничтожение материальных носителей и подлежащие хранению у ответственного пользователя СКЗИ.

16.2. Основанием для уничтожения ключей является истечение срока их действия, вывод из эксплуатации СКЗИ, увольнение сотрудника, снятие с сотрудника обязанностей, связанных с использованием СКЗИ и т.д.

16.3. Неиспользуемые или выведенные из действия ключевые носители подлежат возращению ответственному пользователю СКЗИ либо криптоключи, записанные на них, подлежат уничтожению на месте.

16.4. Уничтожение криптоключей производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей без повреждения ключевого носителя.

16.5. Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков, Smart Card и т.п.).

16.6. Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируется эксплуатационной и технической документацией к соответствующем СКЗИ, а также указаниями организаций, производивших запись криптоключей.

16.7. Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановление ключевой информации.

16.8. Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируется эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей.

16.9. Ключевые документы должны уничтожаться в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ.

16.10. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее десяти дней после вывода их из действия.

16.11. В эти же сроки с отметкой в соответствующем журнале подлежат уничтожению разовые ключевые носители и ранее введенная, и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам. Хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

16.12. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под подпись в соответствующем журнале.

16.13. Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным пользователем СКЗИ с указанием отметки о факте уничтожения в соответствующем журнале поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом.

При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи.

16.14. После уничтожения пользователи СКЗИ должны уведомить об этом ответственного пользователя СКЗИ.

16.15. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожают путем сжигания или с помощью любых бумагорезательных машин. Определенные к уничтожению СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали.

При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к ним процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

16.16. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений.

При этом информация, которая может оставаться в устройствах памяти оборудования должна быть надежно удалена.

16.17. Факт уничтожения носителей эксплуатационной и технической документации, установочных носителей СКЗИ, криптоключей, путем уничтожения ключевых носителей фиксируется в Акте уничтожения.

16.18. Уничтожение производится комиссией в составе не менее трех человек из числа пользователей СКЗИ.

16.19. В акте указывается, что уничтожается и в каком количестве, а также делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых инсталлирующих носителей СКЗИ, эксплуатационной и технической документации к ним.

16.20. Акт уничтожения подлежит хранению у ответственного пользователя СКЗИ.

16.21. Факт уничтожения криптоключей с ключевого носителя совместно с деинсталляцией СКЗИ с его рабочего места фиксируется в Акте деинсталляции СКЗИ.

16.22. Акт деинсталляции СКЗИ подлежит хранению у ответственного пользователя СКЗИ. О факте уничтожении делаются отметки в соответствующем журнале поэкземплярного учета.