МЧС РОССИИ

**ФЕДЕРАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР
ФЕДЕРАЛЬНОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ»**

ПРИКАЗ

15.02.21 г. Краснодар № 51

**Об информационной безопасности в
ФАУ ДПО Краснодарский учебный центр ФПС**

В соответствие с Федеральными законами от 27 июля 2006 года № 149-ФЗ, «Об информации, информационных технологиях и защите информации», от 07 июля 2013 года №112-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и защите информации», от 27 июля 2006 года №152- ФЗ «О персональных данных» Указами Президента Российской Федерации от 5 декабря 2016 года №646 «Об утверждении Доктрины информационной безопасности Российской Федерации, от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», приказом Федеральной службы безопасности от 10.07.2014 года № 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», приказом МЧС России от 10.02.2020 № 79 ДСП «Об утверждении Перечня сведений, составляющих служебную информацию ограниченного распространения Министерства Российской Федерации по делам гражданской обороны чрезвычайных ситуаций и ликвидации последствий стихийных бедствий, в целях повышения эффективности мероприятий по защите информации от несанкционированного доступа на объектах вычислительной техники, п р и к а з ы в а ю:

1. Определить:

1.1. Порядок информационной безопасности учебного центра (приложение №1).

1.2. Инструкцию ответственному за обеспечение требований по технической защите информации в учебном центре (приложение№ 2).

1.3 Инструкцию ответственному за методическое руководство и контроль за эффективностью предусмотренных мер защиты информации в учебном центре (приложение № 3).

1.4. Инструкцию ответственному за организацию обработки и обеспечения безопасности информации объектов информатизации в учебном центре (приложение № 4).

1.5. Инструкцию ответственному за организацию обработки и обеспечения безопасности информации ограниченного распространения объектов информатизации структурных подразделений учебного центра (приложение № 5).

1.6. Инструкцию администратора безопасности информации в учебном центре (приложение № 6).

1.7. Инструкцию администратора безопасности информации ограниченного распространения объектов информатизации в учебном центре (приложение № 7).

1.8. Инструкцию по порядку учета и хранению носителей информации в учебном центре (приложение № 8);

1.9. Инструкцию по порядку организации парольной и антивирусной защиты в учебном центре (приложение № 9).

1.10. Формы журналов, использующихся при организации информационной безопасности в учебном центре (приложение № 10).

2. Приказ довести до всего личного состава учебного центра.

3. Контроль, за выполнением настоящего приказа оставляю за собой.

Начальник учебного центра А.П. Михайлов

Приложение № 1
к приказу Начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02 22г № 51

ПОРЯДОК
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ФАУ ДПО КРАСНОДРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет порядок обеспечения информационной безопасности (далее – Порядок).

1.2. Настоящий Порядок является распорядительным документом учебного центра, устанавливает принципы построения системы информационной безопасности в информационно-телекоммуникационной сети (далее – ИТС) учебного центра с целью обеспечения требуемого уровня безопасности, обрабатываемой в ней информации, не содержащей сведений, составляющих государственную тайну.

1.3. Настоящий Порядок предназначен для работников учебного центра.

1.4. Настоящая Порядок должен служить нормативно-методическим материалом при формулировании требований по обеспечению безопасности информации в учебном центре.

1.5. Настоящий Порядок не исключает необходимости выполнения требований, действующих федеральных нормативных правовых актов, Российских и международных стандартов, устанавливающих требования к обеспечению безопасности и разработке автоматизированных систем.

1.6. Настоящий Порядок разработан в соответствии с требованиями:

1.6.1. Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

1.6.2. Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

1.6.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.6.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации».

1.6.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

1.6.6. Указа Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

1.6.7. Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

1.6.8. Постановления Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

1.6.9. Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.6.10. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «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».

1.6.11. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.6.12. Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.6.13. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.6.14. Приказа ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.7. Действие настоящего Порядка распространяется на любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств.

1.8. Настоящий Порядок подлежит пересмотру и, при необходимости, актуализации в случае изменений в законодательстве Российской Федерации.

2. ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ 3. УЧЕБНОГО ЦЕНТРА

3.1. Информационно-телекоммуникационная сеть учебного центра состоит из двух функционально самостоятельных контуров:

1.1.1. внутренний (служебный) контур – ведомственная цифровая сеть передачи данных «Интранет» (далее – ВЦСПД «Интранет»);

1.1.2. внешний (публичный, открытый) контур – сеть передачи данных «Интернет» (далее – СПД «Интернет»);

1.2. Под инфраструктурой в данном случае понимаются информационные ресурсы и информационные системы (далее – ИС) учебного центра, информационные сервисы, программно-технологические (в том числе технические) решения и пользовательские приложения, методы организации и управления,

система защиты информации, должностные лица, а также средства доступа граждан и юридических лиц к информационным ресурсам и ИС.

1.3. Информационно-телекоммуникационная инфраструктура состоит из нескольких функциональных сегментов (компонентов):

1.3.1. Инфраструктура электронного взаимодействия учебного центра с гражданами;

1.3.2. Инфраструктура электронного взаимодействия учебного центра краю с иными организациями;

2. ПРИНЦИПЫ

2.1. Основным принципом обеспечения информационной безопасности ИТС учебного центра является реализация права на доступ к информации и обеспечения защиты информации от уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

2.2. Основными объектами защиты системы информационной безопасности в ИТС учебного центра являются:

2.2.1. Информационные ресурсы, относящиеся в соответствии с действующими федеральными нормативными правовыми актами к конфиденциальной информации, включая персональные данные, а также общедоступные информационные ресурсы, необходимые для обеспечения функций и реализации полномочий учебного центра;

2.2.2. Информационно-телекоммуникационная сеть учебного центра, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;

2.2.3. Средства доступа граждан и юридических лиц к информационным ресурсам и информационным системам.

2.3. Перечень защищаемых информационных ресурсов определяется внутренними организационно-распорядительными документами учреждения.

3. ЦЕЛИ И ЗАДАЧИ

3.1. Основной целью деятельности по обеспечению информационной безопасности ИТС учебного центра является снижение угроз информационной безопасности до уровня обеспечивающего реализацию полномочий в сфере основной деятельности учебного центра.

3.2. Основными задачами деятельности по обеспечению информационной безопасности ИТС учебного центра являются:

3.2.1. Выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

3.2.2. Предотвращение нарушения требований информационной безопасности;

3.2.3. Исключение, либо минимизация выявленных угроз.

4. УГРОЗЫ

4.1. Целью определения угроз информационной безопасности является установление возможного нарушения конфиденциальности, целостности или доступности информации, содержащейся в ИТС (ИС) учебного центра, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора, а в случае обработки персональных данных и для субъектов персональных данных.

4.2. Определение угроз безопасности информации должно носить систематический характер и осуществляться как на этапе создания элементов ИТС (ИС) и формирования требований по их защите, так и в ходе их эксплуатации. Систематический подход к определению угроз безопасности информации необходим для того, чтобы определить потребности в конкретных требованиях к защите информации и создать адекватную эффективную систему защиты информации в ИС. Меры защиты информации, принимаемые обладателем информации и оператором ИС, должны обеспечивать эффективное и своевременное выявление и блокирование (нейтрализацию) угроз безопасности информации, в результате реализации которых возможно наступление неприемлемых негативных последствий (ущерба).

4.3. В обобщенном виде угрозы безопасности информации характеризуется источниками угроз, факторами, обуславливающими возможность реализации угроз, способами (методами) реализации угроз и последствиями от реализации угроз безопасности информации.

4.4. В качестве источников угроз безопасности информации могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

4.5. Источники угроз безопасности информации являются определяющим фактором при определении угроз безопасности информации в ИС.

4.6. Источники угроз безопасности информации могут быть следующих типов:

4.6.1. Антропогенные источники (антропогенные угрозы);

4.6.2. Техногенные источники (техногенные угрозы);

4.6.3. Стихийные источники (угрозы стихийных бедствий, иных природных явлений).

4.7. В качестве источников антропогенных угроз безопасности информации могут выступать:

4.7.1. Лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в ИС, или нарушения функционирования ИС или обслуживающей ее инфраструктуры, в силу умышленных действий, связанных с корыстными, идейными или иными устремлениями людей (преднамеренные угрозы безопасности информации);

4.7.2. Лица, имеющие доступ к ИС, не преднамеренные (неумышленные) действия (ошибки и т.п.) которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

4.8. Для ИС, в которых целью защиты является обеспечение целостности и доступности обрабатываемой информации, в обязательном порядке подлежат оценке техногенные угрозы, связанные с отказами или сбоями в работе технических средств или программного обеспечения. Такие угрозы могут быть обусловлены:

4.8.1. Низким качеством (надежностью) технических, программных или программно-технических средств;

4.8.2. Низким качеством (надежностью) сетей связи и (или) услуг связи;

4.8.3. Отсутствием или низкой эффективностью систем резервирования или дублирования программно-технических и технических средств;

4.8.4. Низким качеством (надежностью) инженерных систем (кондиционирования, электроснабжения, охранных систем и т.д.);

4.8.5. Низким качеством обслуживания со стороны обслуживающих организаций и лиц.

4.9. Возникновение стихийных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

4.10. К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и прочие, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

4.11. Пересмотр (переоценка) угроз безопасности информации, как минимум, осуществляется в случаях:

4.11.1. Изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регламентирующих защиту информации;

4.11.2. Изменения конфигурации (состава основных компонентов) и особенностей функционирования информационной системы, следствием которых стало возникновение новых угроз безопасности информации;

4.11.3. Выявления уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих;

4.11.4. Появления сведений и фактов о новых возможностях нарушителей.

5. МОДЕЛЬ НАРУШИТЕЛЯ

5.1. Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными

характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

5.2. Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью (разделом) модели угроз безопасности информации и содержит:

5.2.1. Типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации;

5.2.2. Цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации;

5.2.3. Возможные способы реализации угроз безопасности информации.

6. ТИПЫ НАРУШИТЕЛЕЙ

6.1. Типы нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам ИС, а также анализа возможностей нарушителей по доступу к компонентам ИС исходя из структурно-функциональных характеристик и особенностей функционирования ИС.

6.2. В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам ИС и (или) содержащейся в них информации или не иметь такого доступа.

6.3. Анализ прав доступа проводится, как минимум, в отношении следующих компонент ИС:

6.3.1. Устройств ввода/вывода (отображения) информации;

6.3.2. Беспроводных устройств;

6.3.3. Программных, программно-технических и технических средств обработки информации;

6.3.4. Съемных машинных носителей информации;

6.3.5. Машинных носителей информации, выведенных из эксплуатации;

6.3.6. Активного (коммутационного) и пассивного оборудования каналов связи;

6.3.7. Каналов связи, выходящих за пределы контролируемой зоны.

6.4. С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

6.4.1. Внешние нарушители (**тип I**) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

6.4.2. Внутренние нарушители (**тип II**) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

6.5. Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. При оценке возможностей внутренних

нарушителей необходимо учитывать принимаемые оператором организационные меры по допуску субъектов к работе в ИС. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к ИС и ее компонентам, а также мер по контролю за доступом и работой этих лиц.

6.6. Внешнего нарушителя необходимо рассматривать в качестве актуального во всех случаях, когда имеются подключения ИС к внешним ИТС и (или) имеются линии связи, выходящие за пределы контролируемой зоны, используемые для иных подключений.

7. ВИДЫ И ПОТЕНЦИАЛ НАРУШИТЕЛЕЙ

7.1. Угрозы безопасности информации в ИС могут быть реализованы следующими видами нарушителей:

7.1.1. Специальные службы иностранных государств (блоков государств);

7.1.2. Террористические, экстремистские группировки;

7.1.3. Преступные группы (криминальные структуры);

7.1.4. Внешние субъекты (физические лица);

7.1.5. Разработчики, производители, поставщики программных, технических и программно-технических средств;

7.1.6. Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

7.1.7. Лица, обеспечивающие функционирование ИС или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

7.1.8. Пользователи ИС;

7.1.9. Администраторы безопасности;

7.1.10. Ответственные за объекты информатизации;

7.1.11. Бывшие сотрудники (пользователи).

7.2. Виды нарушителей, характерных для информационной системы с заданными структурно-функциональными характеристиками и особенностями функционирования, определяются на основе предположений (прогноза) о возможных целях (мотивации) при реализации угроз безопасности информации этими нарушителями.

7.3. В качестве возможных целей (мотивации) реализации нарушителями угроз безопасности информации в ИС могут быть:

7.3.1. Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;

7.3.2. Реализация угроз безопасности информации по идеологическим или политическим мотивам;

7.3.3. Организация террористического акта;

7.3.4. Причинение имущественного ущерба путем мошенничества или иным преступным путем;

7.3.5. Дискредитация или дестабилизация деятельности органов государственной власти, организаций;

7.3.6. Получение конкурентных преимуществ;

7.3.7. Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;

7.3.8. Любопытство или желание самореализации;

7.3.9. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;

7.3.10. Реализация угроз безопасности информации из мести;

7.3.11. Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий.

7.4. Предположения о целях (мотивации) нарушителей делаются с учетом целей и задач ИС, вида обрабатываемой информации, а также с учетом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации.

7.5. Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в ИС с заданными структурно-функциональными характеристиками и особенностями функционирования.

7.6. В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

7.6.1. Нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в ИС;

7.6.2. Нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в ИС;

7.6.3. Нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в ИС.

8. ВОЗМОЖНЫЕ СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ

8.1. Целью определения возможных способов реализации угроз безопасности информации является формирование предположений о возможных сценариях реализации угроз безопасности информации, описывающих последовательность (алгоритмы) действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз безопасности информации.

8.2. Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования ИС.

8.3. Угрозы безопасности информации могут быть реализованы нарушителями за счет:

8.3.1. Несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чип сетах));

8.3.2. Несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

8.3.3. Несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

8.3.4. Несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

8.3.5. Несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

8.3.6. Воздействия на пользователей, администраторов безопасности, ответственных за объекты информатизации или обслуживающий персонал (социальная инженерия).

9. ОСНОВНЫЕ ПОЛОЖЕНИЯ

9.1. Требования по обеспечению информационной безопасности ИТС учебного центра обязательны к соблюдению всеми его должностными лицами.

9.2. Неисполнение или некачественное исполнение обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к ИС, а также применение к виновным мер в соответствии с требованиями действующего законодательства.

9.3. С целью реализации мероприятий по обеспечению безопасности информации, не составляющей государственную тайну, в учебном центре назначены ответственные должностные лица.

9.4. Руководство учебного центра обеспечивает регулярное повышение квалификации этих лиц.

9.5. Организация и обеспечение защиты информации, не составляющей государственную тайну, обрабатываемой в компонентах ИТС (ИС) в учебном центре возлагается на администратора безопасности.

10. ОСНОВНЫЕ ТРЕБОВАНИЯ

10.1. Требования по обеспечению информационной безопасности в ИТС должны быть взаимосвязаны и представлять собой непрерывный по задачам, подсистемам, уровням и стадиям жизненного цикла (далее – ЖЦ) компонентов ИТС комплекс мероприятий.

10.2. Требования к системе обеспечения информационной безопасности ИТС учебного центра должны быть сформулированы, в том числе по следующим направлениям:

10.2.1. Назначение и распределение ролей должностных лиц структурных подразделений;

10.2.2. Обеспечение информационной безопасности компонентов ИТС (ИС) на стадиях ЖЦ;

10.2.3. Защита от несанкционированного доступа (далее – НСД), управления доступом и регистрацией действий в ИС;

10.2.4. Антивирусная защита;

10.2.5. Использование ресурсов ВЦСПД «Интранет» и СПД «Интернет»;

10.2.6. Использование средств криптографической защиты информации;

10.2.7. Использование электронной подписи;

10.2.8. Защита персональных данных;

10.2.9. Защита основных компонентов ИТС (ИС).

11. ОБЩИЕ ТРЕБОВАНИЯ ПРИ НАЗНАЧЕНИИ И РАСПРЕДЕЛЕНИИ ОБЯЗАННОСТЕЙ

11.1. Для обеспечения эффективного функционирования компонентов ИТС должны быть определены соответствующие обязанности должностных лиц учебного центра.

11.2. Формирование и назначение обязанностей должностных осуществлять с учетом соблюдения принципа предоставления минимальных прав и полномочий, необходимых для выполнения должностных обязанностей.

11.3. Обязанности персонифицировать с установлением ответственности за их выполнение.

11.4. Ответственность должна быть зафиксирована в должностных инструкциях или организационно-распорядительных документах структурных подразделений.

11.5. С целью предупреждения возникновения и снижения рисков нарушения информационной безопасности не рекомендуется совмещение одного сотрудника функций пользователя и администратора.

11.6. Должны быть определены, выполняться и регистрироваться процедуры контроля деятельности должностных лиц, обладающих совокупностью полномочий, определяемых их обязанностями, позволяющими получить контроль над защищаемым информационным ресурсом.

11.7. Должны быть определены, выполняться и регистрироваться процедуры приема на работу, влияющие на обеспечение информационной безопасности и включающие:

11.7.1. Проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;

11.7.2. Проверку в части знаний и навыков в области обеспечения информационной безопасности, оценку профессиональной пригодности.

11.8. Указанные процедуры должны предусматривать фиксацию результатов проводимых проверок.

11.9. Рекомендуется определить, выполнять и регистрировать с фиксацией результатов процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности должностных лиц в области обеспечения информационной безопасности, а также внеплановой проверки - при выявлении

фактов их нештатного поведения, участия в инцидентах информационной безопасности или подозрений в таком поведении или участии.

11.10. Все должностные лица, работающие с конфиденциальной информацией, должны давать письменное обязательство о соблюдении конфиденциальности. При этом условие о соблюдении конфиденциальности должно распространяться на всю защищаемую информацию, доверенную должностному лицу или ставшую ему известной в процессе выполнения им своих должностных обязанностей.

11.11. При взаимодействии с внешними организациями требования по обеспечению информационной безопасности должны регламентироваться положениями, включаемыми в договоры (соглашения) с ними.

11.12. Обязанности должностных лиц по выполнению требований по обеспечению информационной безопасности должны включаться в служебные (трудовые) контракты (соглашения, договоры) и (или) должностные инструкции.

12. ОБЩИЕ ТРЕБОВАНИЯ К ОСНОВНЫМ КОМПОНЕНТАМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

12.1. В информационных системах, реализующих компоненты ИТС учебного центра, информация классифицируется как:

12.1.1. Общедоступная;

12.1.2. Конфиденциальная.

12.2. Каждому виду информации соответствует свой необходимый уровень защиты (свой набор требований по защите).

12.3. В качестве объектов защиты должны рассматриваться:

12.3.1. Информационные ресурсы;

12.3.2. Управляющая информация ИС;

12.3.3. Информационный технологический процесс;

12.3.4. Объекты информатизации.

12.4. Учебный центр, в части касающейся защиты информации, несёт ответственность за:

12.4.1. Достоверность информации, официально предоставляемой внешним организациям и гражданам;

12.4.2. Достоверность и выполнение регламента предоставления внешним организациям и гражданам информации, обязательность и порядок предоставления которой определены законодательством Российской Федерации и/или нормативными учебного центра или соглашением сторон;

12.4.3. Обеспечение соответствующего законодательству Российской Федерации уровня защиты, как собственной информации, так и информации, официально полученной из внешних организаций и от граждан.

12.5. Допускается совмещение выполнения указанных функций с другими обязанностями.

12.6. Администратор безопасности должен иметь служебные полномочия по настройке параметров системы, определяющих полномочия пользователей по доступу к информации.

12.7. Администратор безопасности должен иметь право добавлять в систему нового пользователя, а также удалять из системы такого пользователя, но с обязательным предварительным согласованием устанавливаемых прав доступа пользователей к информации с ответственным за организацию обработки и обеспечение безопасности.

12.8. Устанавливаемые права доступа к информации назначаются начальником учебного центра.

12.9. Информационная безопасность обеспечивается на всех стадиях ЖЦ компонентов ИТС (ИС), с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений, администраторов систем и конечных пользователей).

12.10. Стадии и этапы создания компонентов ИТС (ИС) описываются в соответствующих комплексах стандартов на автоматизированные системы.

12.11. Защита информации, содержащейся в ИС, является составной частью работ по созданию и эксплуатации ИС и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в ИС, в рамках системы (подсистемы) защиты информации ИС (далее – СЗИ ИС).

12.12. Организационные и технические меры защиты информации, реализуемые в рамках СЗИ ИС, в зависимости от информации, содержащейся в ИС, целей создания ИС и задач, решаемых этой ИС, направлены на исключение:

12.12.1. Неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

12.12.2. Неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

12.12.3. Неправомерного блокирования информации (обеспечение доступности информации).

12.13. Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

12.13.1. Формирование требований к защите информации, содержащейся в ИС;

12.13.2. Внедрение СЗИ ИС;

12.13.3. Аттестация по требованиям защиты информации (далее - аттестация) и ввод ее в эксплуатацию;

12.13.4. Обеспечение защиты информации в ходе эксплуатации;

12.14. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

12.15. Выполнение работ на всех стадиях жизненного цикла компонентов ИТС (ИС) в части вопросов обеспечения информационной безопасности должно осуществляться по согласованию и под контролем администратора безопасности.

12.16. Эксплуатируемые ИС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных в ИС защитных мер, в том числе описание состава и требований к реализации организационных защитных мер, состава и требований к эксплуатации технических защитных мер.

12.17. В договор (контракт) о поставке готовых СЗИ ИС и их компонентов должна включаться сопутствующая документация по сопровождению поставляемых изделий на весь срок их службы.

12.18. В случае невозможности включения в договор (контракт) сопутствующей документации, должен быть приобретен полный комплект документации, обеспечивающий возможность сопровождения СЗИ ИС и их компонентов без участия разработчика.

12.19. На стадии эксплуатации компонентов ИТС (ИС) должны быть определены, выполняться и регистрироваться процедуры:

12.19.1. Контроля работоспособности (функционирования, эффективности) реализованных в ИС защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер;

12.19.2. Контроля отсутствия уязвимостей в оборудовании и программном обеспечении ИС;

12.19.3. Контроля внесения изменений в параметры настройки ИС и применяемых технических защитных мер;

12.19.4. Контроля необходимого обновления программного обеспечения ИС, включая программное обеспечение технических защитных мер.

12.20. На стадии эксплуатации компонентов ИТС (ИС) должны быть определены, выполняться и регистрироваться процедуры контроля состава, устанавливаемого и (или) используемого программного обеспечения.

12.21. Должны быть определены, выполняться и контролироваться процедуры, необходимые для обеспечения сохранности носителей информации.

12.22. На стадии сопровождения (модернизации) компонентов ИТС (ИС) должны быть определены, выполняться и регистрироваться процедуры контроля, обеспечивающие защиту от:

12.22.1. Умышленного и неумышленного несанкционированного раскрытия, модификации или уничтожения информации;

12.22.2. Отказа в обслуживании или ухудшения обслуживания.

13. ОБЩИЕ ТРЕБОВАНИЯ ПРИ УПРАВЛЕНИИ ДОСТУПОМ И РЕГИСТРАЦИИ

13.1. В составе ИС должны применяться защитные меры от НСД и нерегламентированных действий (далее – НРД), а также средства защиты информации, сертифицированные по требованиям безопасности информации.

13.2. Защитные меры от НСД должны обеспечивать сокрытие вводимых субъектами доступа аутентификационных данных на устройствах отображения информации.

13.3. Размещение устройств отображения информации должно препятствовать ее несанкционированному просмотру.

13.4. Должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры:

13.4.1. Идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются должностными лицами Главного управления МЧС России по Краснодарскому краю, и программных процессов (сервисов);

13.4.2. Разграничения доступа к информационным ресурсам на основе ролевого метода, с определением для каждой роли полномочий по доступу к информационным ресурсам;

13.4.3. Управления предоставлением/отзывом и блокированием доступа;

13.4.4. Регистрации действий субъектов доступа с обеспечением контроля целостности и защиты данных регистрации;

13.4.5. Управления идентификационными данными, аутентификационными данными и средствами аутентификации;

13.4.6. Управления учетными записями субъектов доступа;

13.4.7. Ограничения действий пользователей по изменению настроек их автоматизированных рабочих мест (далее – АРМ), в том числе использование ограничений на изменение BIOS;

13.4.8. Ограничения действий пользователей по изменению параметров настроек ИС;

13.4.9. Выявления и блокирования несанкционированного перемещения и копирования информации;

13.4.10. Исключение использования технологий беспроводного доступа к информации;

13.4.11. Использования мобильных устройств для доступа к информации в случае их применения.

13.5. Должно быть реализовано ведение электронных журналов действия и операций автоматизированных рабочих мест, серверного и сетевого оборудования, межсетевых экранов и ИС с целью их использования при реагировании на инциденты информационной безопасности.

13.6. Система управления доступом, регистрации и учета может быть реализована с помощью штатных средств ИС (операционных систем, приложений и СУБД) и/или использовать сертифицированные или разрешенные к применению средства защиты информации от НСД.

13.7. Использование биометрических и технических (с помощью электронных ключей или ЭП) мер аутентификации для некоторых компонентов ИТС.

13.8. Должен быть определен, выполняться, регистрироваться и контролироваться порядок доступа к защищенным объектам информатизации.

13.9. Должны быть определены и доведены до сведения должностных лиц учебного центра процедуры, определяющие действия в случае компрометации информации, необходимой для их идентификации, аутентификации и (или) авторизации, в том числе произошедшей по их вине, включая информацию о способах распознавания таких случаев.

13.10. При увольнении или изменении должностных обязанностей должностных лиц, имевших доступ к информации, необходимой для идентификации, аутентификации и (или) авторизации пользователей компонентов ИТС (ИС), необходимо выполнить регламентированные процедуры соответствующего пересмотра прав доступа.

13.11. Работа всех должностных лиц (пользователей, администраторов и т.п.) в сети ИТС должна осуществляться под уникальными и персонифицированными учетными записями.

14. ОБЩИЕ ТРЕБОВАНИЯ ПРИ РАБОТЕ С ПРОГРАММНЫМИ СРЕДСТВАМИ

14.1. На всех автоматизированных рабочих местах и серверах, образующих компоненты ИТС учебного центра, должны применяться средства антивирусной защиты.

14.2. Должны быть определены, выполняться и контролироваться процедуры установки и регулярного обновления средств антивирусной защиты на автоматизированных рабочих местах и серверах.

14.3. Рекомендуется организовать функционирование постоянной антивирусной защиты в автоматическом режиме и автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных.

14.4. Отключение или невыполнение процедур обновления антивирусных средств не допускается.

14.5. Использование съемных носителей информации должно быть регламентировано с обязательной их проверкой средствами антивирусной защиты.

14.6. При обеспечении антивирусной защиты должны быть разработаны и введены в действие инструкции по антивирусной защите.

14.7. Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

14.8. После изменения программного обеспечения должна быть выполнена антивирусная проверка.

14.9. На рабочих местах компонентов ИТС не допускается установка и использование программного обеспечения, не связанного с выполнением конкретных функций в технологических процессах ИТС.

14.10. Должны быть определены, выполняться и контролироваться процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать:

14.10.1. Необходимые меры по отражению и устранению последствий вирусной атаки;

14.10.2. Порядок официального информирования руководства;

14.10.3. Порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

14.11. Контроль за установкой и обновлением антивирусных средств должен быть возложен на должностных лиц, назначенных администраторами безопасности.

14.12. Ответственность за организацию выполнения требований по антивирусной защите должна быть возложена на администратора безопасности

14.13. Обязанности по выполнению предписанных мер антивирусной защиты должны быть возложены на каждое должностное лицо, имеющего доступ к автоматизированному рабочему месту и (или) ИС.

15. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ РЕСУРСОВ СПД «ИНТЕРНЕТ»

15.1. Ресурсы СПД «Интернет» учебным центром используются для получения и распространения информации, связанной с профессиональной деятельностью, информационно-аналитической работой, обмена сообщениями, а также ведения межведомственного информационного взаимодействия.

15.2. Иное использование ресурсов сети Интернет должно рассматриваться как нарушение информационной безопасности.

15.3. В связи с повышенными рисками информационной безопасности при взаимодействии с СПД «Интернет», должны применяться соответствующие средства защиты информации, обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

15.4. Предназначенные для этого средства защиты информации, в том числе шифровальные (криптографические) средства, должны пройти сертификацию в установленном законодательством Российской Федерации порядке.

15.5. В учреждении должна быть разработана и введена в действие инструкция и по использованию СПД «Интернет».

15.6. Почтовый обмен через сеть Интернет должен осуществляться с использованием защитных мер, включая антивирусную защиту.

15.7. Для обнаружения компьютерных атак необходимо использовать системы обнаружения вторжений, реализованные программными или программно-аппаратными средствами.

15.8. Использование сети Интернет должно быть санкционировано начальником учебного центра.

16. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

16.1. Средства криптографической защиты информации (далее - СКЗИ) предназначены для защиты информации при ее обработке, хранении и передаче по каналам связи.

16.2. Применение СКЗИ должно проводиться в соответствии с моделью угроз и моделью нарушителя.

16.3. Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с законодательством РФ, нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

16.4. Для обеспечения безопасности необходимо использовать СКЗИ, которые:

16.4.1. Допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

16.4.2. Сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

16.5. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ должны осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам.

16.6. Должен быть определен и утвержден реестр должностных лиц, имеющих доступ к ключевой информации.

16.7. К работе на АРМ с установленным СКЗИ допускаются только определенные для эксплуатации должностные лица, прошедшие соответствующую подготовку и ознакомленные с пользовательской документацией на СКЗИ, а также другими нормативными документами.

16.8. К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются доверенные должностные лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

16.9. Задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности возлагаются на администратора безопасности.

16.10. Должно быть исключено бесконтрольное проникновение и пребывание в защищенных помещениях, в которых размещаются технические средства АРМ, посторонних лиц, по роду своей деятельности, не допущенных к работе в указанных помещениях.

16.11. В случае необходимости присутствия посторонних лиц в защищенных помещениях, в которых размещаются технические средства АРМ должен быть обеспечен контроль за их действиями.

16.12. Рекомендуется использовать АРМ с СКЗИ в однопользовательском режиме. Не допускается оставлять без контроля АРМ при включенном питании и загруженном программном обеспечении СКЗИ после ввода ключевой информации.

16.13. При уходе с рабочего места пользователь должен выйти со своей учетной записи операционной системы.

16.14. Рекомендуется предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части АРМ, например, опечатывание системного блока АРМ администратором.

16.15. Рекомендуется принять меры по исключению вхождения лиц, не ответственных за администрирование АРМ, в режим конфигурирования BIOS (например, с использованием парольной защиты).

16.16. Рекомендуется определить в BIOS установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM, исключаются прочие нестандартные виды загрузки ОС, включая сетевую загрузку.

16.17. На технических средствах АРМ с установленным СКЗИ необходимо использовать только лицензионное программное обеспечение.

16.18. Использование средств отладки приложений необходимых для технологических потребностей пользователя должно быть санкционировано начальником структурного подразделения.

16.19. Необходимо исключить попадание в систему средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

16.20. Рекомендуется ограничить возможности пользователя запуском только тех приложений, которые разрешены администратором безопасности.

16.21. Рекомендуется разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.).

16.22. Установка и настройка СКЗИ на АРМ должна выполняться в присутствии администратора безопасности.

16.23. Установка СКЗИ на АРМ должна производиться только с дистрибутива, полученного по доверенному каналу.

16.24. Установка СКЗИ и первичная инициализация ключевой информации осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

16.25. При установке ПО СКЗИ на АРМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ.

16.26. Рекомендуется перед установкой произвести проверку ОС на отсутствие вредоносных программ с помощью антивирусных средств.

16.27. По завершении инициализации осуществляются настройка и контроль работоспособности программного обеспечения (далее – ПО).

17. ОБЩИЕ ТРЕБОВАНИЯ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

17.1. Электронная подпись (далее – ЭП) выдаётся уполномоченному должностному лицу и предназначена для использования в ИС, в которых электронные документы признаются эквивалентными их бумажным аналогам.

17.2. Сертификат открытого ключа ЭП выдается удостоверяющим центром по запросу начальника учебного центра.

17.3. В случае компрометации закрытого ключа ЭП владелец сертификата немедленно извещает ответственного за организацию обработки и обеспечение безопасности и администратора безопасности о возникшей ситуации.

17.4. К событиям, связанным с компрометацией ключей, относятся следующие ситуации:

17.4.1. Утрата ключевых носителей;

17.4.2. Утрата ключевых носителей с их последующим обнаружением;

17.4.3. Увольнение должностных лиц, имевших доступ к ключевой информации;

17.4.4. Нарушение правил хранения и уничтожения закрытого ключа;

17.4.5. Нарушение целостности печатей на сейфах с носителями ключевой информации (если используется процедура опечатывания сейфов);

17.4.6. Утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

17.4.7. Утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

17.4.8. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

17.4.9. Доступ посторонних лиц к ключевой информации.

17.5. Выведенные из действия закрытые ключи ЭП уничтожаются.

17.6. В целях обеспечения безопасности уполномоченные должностные лица обязаны:

17.6.1. Хранить в тайне ключ ЭП (закрытый ключ);

17.6.2. Немедленно требовать приостановления действия с последующим аннулированием сертификата, если тайна закрытого ключа ЭП нарушена;

17.6.3. Участвовать в плановой смене сертификатов ключей подписи;

17.6.4. Оказывать содействие в работе комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных, используемых в учебном центре при рассмотрении спорных вопросов и конфликтных ситуаций, его касающихся.

17.7. Должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации, который должен исключать возможность несанкционированного доступа к ним.

17.8. Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

17.9. Запрещается:

17.9.1. Снимать несанкционированные администратором безопасности копии с ключевых носителей;

17.9.2. Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей (монитор) АРМ или принтер;

17.9.3. Устанавливать ключевой носитель в считывающее устройство АРМ в режимах, не предусмотренных функционированием системы, а также устанавливать носитель в другие АРМ;

17.9.4. Записывать на ключевой носитель постороннюю информацию;

17.9.5. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

18. ОБЩИЕ ТРЕБОВАНИЯ ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

18.1. Обработка персональных данных должна производиться в соответствии с требованиями нормативных и методических документов регуляторов.

18.2. Для осуществления деятельности по обработке персональных данных, (далее - ПДн) должны быть:

18.2.1. Установлены цели обработки ПДн;

18.2.2. Установлена необходимость осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн и организована деятельность по своевременному направлению указанного уведомления в соответствии с требованиями Федерального закона в случае наличия такой необходимости;

18.3. Для каждого ресурса ПДн должно быть обеспечено:

18.3.1. Установление цели обработки ПДн;

18.3.2. Установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;

18.3.3. Определение перечня и категорий, обрабатываемых ПДн;

18.3.4. Выполнение процедур учета количества субъектов ПДн;

18.3.5. Выполнение ограничения обработки ПДн достижением цели обработки;

18.3.6. Соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;

18.3.7. Точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки;

18.3.8. Выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона;

18.3.9. Выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона;

18.3.10. Прекращение обработки и уничтожение или обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных Федеральным законом.

18.4. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета лиц, имеющих доступ к ПДн.

18.5. Документ, определяющий перечень лиц, имеющих доступ к ПДн, утверждается начальником учебного центра.

18.6. Обработка ПДн должностными лицами должна осуществляться только с целью выполнения должностных обязанностей.

18.7. Должны быть определены, выполняться и контролироваться процедуры ознакомления должностных лиц, осуществляющих обработку ПДн, с положениями законодательства Российской Федерации и внутренними документами, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

18.8. Должны быть определены, выполняться и контролироваться процедуры учета помещений, в которых осуществляется обработка ПДн, а также доступа лиц в помещения, в которых ведется обработка ПДн.

18.9. При работе с материальными носителями ПДн должно быть обеспечено:

18.9.1. Обособление ПДн от иной информации, в частности, путем фиксации их на отдельных съемных носителях ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях);

18.9.2. Учет съемных носителей ПДн;

18.9.3. Установление, выполнение и контроль выполнения порядка хранения съемных, в том числе машинных, носителей ПДн и доступа к ним;

18.9.4. Хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных съемных носителях;

18.9.5. Регистрация и учет мест хранения материальных носителей ПДн с фиксацией категории обрабатываемых персональных данных включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями;

18.9.6. Назначение должностных лиц, ответственных за организацию хранения материальных носителей ПДн;

18.9.7. Установление и выполнение порядка уничтожения информации с машинных носителей ПДн.

18.10. Поручение обработки ПДн третьему лицу (далее - обработчик) должно осуществляться на основании договора.

18.11. В договоре должны быть определены перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки, должна быть установлена обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн.

18.12. При поручении обработки персональных данных обработчику необходимо получить согласие субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

18.13. Должно быть назначено лицо, ответственное за организацию обработки и обеспечение безопасности ПДн.

18.14. Полномочия лица, ответственное за организацию обработки и обеспечение безопасности ПДн, а также его права и обязанности должны быть установлены руководящими документами.

18.15. При необходимости официального обмена ПДн с внешними организациями необходимо применять защищённые каналы передачи информации, использующие криптографические средства защиты информации и ЭП.

19. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

19.1. Своевременное реагирование на инциденты информационной безопасности является одним из необходимых условий минимизации последствий нерегламентированных воздействий на компоненты ИТС (ИС).

19.2. При планировании деятельности, направленной на реагирование на инциденты информационной безопасности, наряду с настоящей Политикой необходимо руководствоваться действующими стандартами, содержащими требования к системе менеджмента информационной безопасности.

19.3. Основными этапами процесса реагирования на инциденты информационной безопасности являются:

19.3.1. Подготовка к факту возникновения инцидента информационной безопасности и принятие превентивных мер;

19.3.2. Обнаружение и регистрация инцидента информационной безопасности;

19.3.3. Начальное реагирование на инцидент информационной безопасности;

19.3.4. Формирование стратегии реагирования на инцидент информационной безопасности;

19.3.5. Восстановление штатного функционирования компонентов ИТС (ИС), подвергшихся влиянию инцидента информационной безопасности;

19.3.6. Расследование инцидента;

19.3.7. Составление отчета;

19.3.8. Выработка решения.

19.4. Первопричиной наступления события инцидента информационной безопасности является потенциальная способность злоумышленника получить необоснованные привилегии для доступа к защищенной информации.

19.5. Предположение о том, что произошёл инцидент информационной безопасности, как правила, базируется на:

19.5.1. Одновременных сообщениях об инциденте информационной безопасности из нескольких источников (пользователи, система обнаружения вторжений, журнальные файлы (logfiles));

19.5.2. Сообщениях системы обнаружения вторжений о множественном повторяющемся событии;

19.5.3. Анализе журнальных файлов автоматизированной системы;

19.6. Признаки инцидента делятся на две основные категории:

19.6.1. Сообщения о том инцидент происходит в настоящий момент;

19.6.2. Сообщения о том, что инцидент, возможно, произойдёт в скором будущем.

19.7. Основными признаками совершающегося инцидента являются:

19.7.1. Фиксация переполнение буфера системы обнаружения вторжений;

19.7.2. Уведомление антивирусной программы;

19.7.3. Отключение WEB – интерфейса;

19.7.4. Фиксация низкой пропускной способности сетевого оборудования;

19.7.5. Фиксация файлов с нечитабельными названиями;

19.7.6. Фиксация множества повторяющихся сообщений;

19.7.7. Фиксация изменения конфигурации оборудования;

19.7.8. Фиксация множественных неудачных попыток авторизации;

19.7.9. Фиксация резкое увеличение сетевого трафика.

19.8. Документирование событий инцидента информационной безопасности необходимо для сбора и последующего обобщения результатов расследования.

19.9. Документированию подлежат все факты и доказательства злонамеренного воздействия.

19.10. Различают технологические и операционные свидетельства воздействия.

19.11. К технологическим свидетельствам относят информацию, полученную от технических средств сбора и анализа данных (анализаторы трафика, системы обнаружения вторжений),

19.12. К операционным свидетельствам относят данные, собранные свидетельства обращений в процессе опроса должностных лиц, пользователей.

19.13. В ходе расследования инцидента все свидетельства должны быть защищены от дискредитации, поскольку данные могут содержать информацию о действенных уязвимостях ИС.

20. ФОРМИРОВАНИЕ СТРАТЕГИИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

20.1. Стратегия реагирования на инцидент информационной безопасности определяет лучший путь реагирования на инцидент.

20.2. Стратегия также определяет, какие действия будут предприняты по факту возникновения инцидента (возбуждение гражданского или уголовного дела, административное воздействие), в зависимости от предполагаемых причин и последствий возникновения инцидента.

20.3. Стратегия является результатом коллективной работы.

21. ВОССТАНОВЛЕНИЕ ШТАТНОГО ФУНКЦИОНИРОВАНИЯ КОМПОНЕНТОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

21.1. Восстановление штатного функционирования компонентов ИТС (ИС) представляет собой последовательность действий разработанных в соответствии с

утвержденным регламентом и напрямую зависит от особенности функционирования ИС и способа атаки, который был применён злоумышленником.

21.2. Масштабы восстановления могут быть различны, от лечения заражённых вирусом файлов и восстановления операционной среды с резервных копий, до отстаивания репутации организации в суде.

22. РАССЛЕДОВАНИЕ ИНЦИДЕНТА

Расследование инцидента безопасности осуществляется в пределах компетенции, а также технических и организационных возможностей учебного центра. Во случаях, возникновения инцидента безопасности, производится уведомление отдела безопасности ГУСБ, через ДОН.

23. ПРОВЕРКА И ОЦЕНКА

23.1. Проверка и оценка информационной безопасности проводится путем выполнения следующих процессов:

23.1.1. Мониторинга информационной безопасности и контроля защитных мер;

23.1.2. Самооценки информационной безопасности;

23.1.3. Аудита информационной безопасности;

23.1.4. Анализа функционирования системы обеспечения информационной безопасности.

23.2. Основными целями мониторинга информационной безопасности и контроля защитных мер являются:

23.2.1. Оперативное и постоянное наблюдение,

23.2.2. сбор, анализ и обработка данных под заданные цели.

23.3. Целями анализа функционирования системы обеспечения информационной безопасности могут быть:

23.3.1. Контроль за реализацией положений внутренних документов по обеспечению информационной безопасности;

23.3.2. Выявление нештатных действий;

23.3.3. Выявление инцидентов информационной безопасности.

23.4. Мониторинг и контроль защитных мер проводится должностными лицами, назначенными администраторами безопасности.

23.5. Анализ функционирования системы обеспечения информационной безопасности (далее – СОИБ) инициируется:

23.5.1. Ответственными за организацию обработки и обеспечение безопасности;

23.5.2. Администраторами безопасности;

23.5.3. Руководством структурного подразделения.

23.6. Основными целями проведения анализа функционирования СОИБ являются:

23.6.1. Оценка эффективности СОИБ;

23.6.2. Оценка соответствия СОИБ требованиям законодательства Российской Федерации и стандартов;

23.6.3. Оценка соответствия СОИБ существующим и возможным угрозам информационной безопасности;

23.6.4. Оценка следования принципам информационной безопасности и выполнения требований по обеспечению информационной безопасности, закрепленным в настоящей Политике, а также в иных внутренних документах.

23.7. Результаты, полученные в ходе анализа функционирования СОИБ, являются среди прочего, основой для совершенствования СОИБ.

24. ОТВЕТСТВЕННОСТЬ

24.1. Общее руководство обеспечением информационной безопасности и ответственность за поддержание положений настоящего Порядка в актуальном состоянии возлагается на ответственного за организацию обработки и обеспечение безопасности информации.

24.2. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

Заместитель начальника учебного центра Е.В.Шевченко

Приложение № 2
к приказу начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.21г. № 57

ИНСТРУКЦИЯ ОТВЕТСТВЕННОМУ ЗА ОБЕСПЕЧЕНИЕ ТРЕБОВАНИЙ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Должностная инструкция ответственному за обеспечение требований по технической защите информации в учебном центре (далее – Инструкция) определяет, обязанности и права лица, назначенного ответственным за обеспечение требований по технической защите информации в учебном центре (далее – ответственный за ТЗИ).

1.2. Инструкция разработана в соответствии с требованиями:

1.2.1. Трудового кодекса Российской Федерации;

1.2.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.2.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

1.2.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.2.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

1.2.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «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»;

1.2.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.2.8. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.3. Ответственный за ТЗИ назначается приказом начальника учебного центра.

2. ФУНКЦИИ

Ответственный за ТЗИ отвечает за:

2.1. Методическое руководство по обеспечению безопасности информации и контроль выполнения требований по обеспечению безопасности информации.

2.2. Соблюдение требований к защите информации.

2.3. Планирование и выполнение работ по противодействию иностранным техническим разведкам (далее – ИТР) и технической защите информации, обрабатываемой средствах вычислительной техники.

2.4. Доведение до ответственных должностных лиц положений законодательства Российской Федерации, правовых актов по вопросам обработки информации, требований к защите информации.

2.5. Организацию осуществления контроля за обработкой информации.

2.6. Организацию осуществления контроля за соблюдением инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей по вопросам защиты информации.

2.7. Взаимодействие с другими организациями (учреждениями).

3. ОБЯЗАННОСТИ

Ответственный за ТЗИ обязан:

3.1. Организовывать контроль планирования и выполнения работ по противодействию иностранным техническим разведкам (далее – ИТР) и технической защите информации, обрабатываемой СВТ.

3.2. Вести методическое руководство по обеспечению безопасности информации и контроль выполнения требований по обеспечению безопасности информации.

3.3. Осуществлять контроль соблюдения требований к защите информации.

3.4. Осуществлять взаимодействие с другими организациями (учреждениями).

3.5. Осуществлять контроль за эффективностью предусмотренных мер защиты информации.

3.6. Организовывать проведение занятий по изучению нормативных правовых и руководящих документов по вопросам защиты информации.

3.7. Обеспечивать проведение служебных расследований по фактам и попыткам нарушения безопасности информации.

3.8. Организовывать обработку и использование информации исключительно в целях, предусмотренных нормативными правовыми актами РФ.

3.9. Организовывать соблюдение безопасности информации требуемому уровню защищенности.

3.10. Осуществлять контроль содержания и объема обрабатываемых информации и соответствия их перечню.

3.11. Осуществлять контроль за соблюдением порядка и условиям применения организационных и технических мер по обеспечению безопасности информации необходимых при обработке и выполнении требований к защите информации,

исполнение которых обеспечивает установленные уровни защищенности информации.

3.12. Осуществлять контроль проведения анализа эффективности применения мер по обеспечению безопасности информации.

4. ПРАВА

Ответственный за ТЗИ имеет право:

4.1. Требовать от должностных лиц выполнения установленных правил обработки информации, инструкций и других нормативных правовых документов по обеспечению безопасности информации.

4.2. Запрашивать у должностных лиц информацию, необходимую для реализации полномочий.

4.3. Организовывать разработку мероприятий по совершенствованию безопасности информации.

4.4. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4.5. Организовывать проверки по контролю соответствия обработки информации требованиям к защите информации.

4.6. Требовать от ответственных должностных лиц уточнения, блокирования или уничтожения недостоверной, или полученной незаконным путем информации.

4.7. Организовывать проведение расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов вычислительной техники.

4.8. Организовывать анализ ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4.9. Принимать предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации при их обработке.

5. ОТВЕТСТВЕННОСТЬ

Ответственный за ТЗИ несёт ответственность в пределах, определённых действующими нормативными документами:

5.1. За ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящим должностным регламентом (должностной инструкцией).

5.2. За неправильность и неполноту использования предоставленных ему прав.

5.3. За правонарушения, совершенные в процессе осуществления своей деятельности.

5.4. За реализацию принятой политики информационной безопасности.

5.5. За разглашение сведений, конфиденциального характера, ставших известными ему по роду работы.

Заместитель начальника учебного центра Е.В.Шевченко

Приложение № 3
к приказу Начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.22г № 51

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОМУ ЗА МЕТОДИЧЕСКОЕ РУКОВОДСТВО И КОНТРОЛЬ ЗА ЭФФЕКТИВНОСТЬЮ ПРЕДУСМОТРЕННЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Должностная инструкция ответственному за методическое руководство и контроль за эффективностью предусмотренных мер защиты информации в учебном центре (далее – Инструкция) определяет, обязанности и права лица, назначенного ответственным за методическое руководство и контроль за эффективностью предусмотренных мер защиты информации в учебном центре (далее – ответственный за МР).

1.2. Инструкция разработана в соответствии с требованиями:

1.2.1. Трудового кодекса Российской Федерации;

1.2.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.2.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

1.2.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.2.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»

1.2.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «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»;

1.2.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.2.8. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.3. Ответственный за МР назначается приказом начальника учебного центра.

2. ФУНКЦИИ

Ответственный за МР отвечает за:

2.1. Методическое руководство по обеспечению безопасности информации и контроль выполнения требований по обеспечению безопасности информации.

2.2. Соблюдение требований к защите информации.

2.3. Доведение до ответственных должностных лиц положений законодательства Российской Федерации, правовых актов по вопросам обработки информации, требований к защите информации.

2.4. Организацию осуществления контроля за соблюдением инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей по вопросам защиты информации.

3. ОБЯЗАННОСТИ

Ответственный за МР обязан:

3.1. Вести методическое руководство по обеспечению безопасности информации и контроль выполнения требований по обеспечению безопасности информации.

3.2. Осуществлять контроль соблюдения требований к защите информации.

3.3. Организовывать проведение занятий по изучению нормативных правовых и руководящих документов по вопросам защиты информации.

3.4. Обеспечивать проведение служебных расследований по фактам и попыткам нарушения безопасности информации.

3.5. Организовывать соблюдение безопасности информации требуемому уровню защищенности.

3.6. Осуществлять контроль за соблюдением порядка и условиям применения организационных и технических мер по обеспечению безопасности информации необходимых при обработке и выполнении требований к защите информации, исполнение которых обеспечивает установленные уровни защищенности информации.

3.7. Осуществлять контроль проведения анализа эффективности применения мер по обеспечению безопасности информации.

4. ПРАВА

Ответственный за МР имеет право:

4.1. Требовать от должностных лиц выполнения установленных правил обработки информации, инструкций и других нормативных правовых документов по обеспечению безопасности информации.

4.2. Запрашивать у должностных лиц информацию, необходимую для реализации полномочий.

4.3. Организовывать разработку мероприятий по совершенствованию безопасности информации.

4.4. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4.5. Требовать от ответственных должностных лиц уточнения, блокирования или уничтожения недостоверной, или полученной незаконным путем информации;

4.6. Организовывать проведение расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов вычислительной техники.

4.7. Принимать предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации при их обработке.

5. ОТВЕТСТВЕННОСТЬ

Ответственный за МР несёт ответственность в пределах, определённых действующими нормативными документами:

5.1. За ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящим должностным регламентом (должностной инструкцией).

5.2. За неправильность и (или) неполноту использования предоставленных ему прав.

5.3. За правонарушения, совершенные в процессе осуществления своей деятельности.

5.4. За реализацию принятой политики информационной безопасности.

5.5. За разглашение сведений, конфиденциального характера, ставших известными ему по роду работы.

Заместитель начальника учебного центра  Е.В.Шевченко

Приложение № 4
к приказу начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.21г № 57

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОМУ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Должностная инструкция ответственному за организацию обработки и обеспечения информации в учебном центре (далее – Инструкция) определяет, обязанности и права лица, назначенного ответственным за организацию обработки и обеспечения безопасности информации в учебном центре (далее – ответственный за БИ).

1.2. Инструкция разработана в соответствии с требованиями:

1.2.1. Трудового кодекса Российской Федерации;

1.2.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.2.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

1.2.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.2.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»

1.2.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «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»;

1.2.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.2.8. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.3. Ответственный за БИ назначается приказом начальника учебного центра.

1.4. Ответственный за БИ в структурных подразделениях учебного центра назначается начальник структурного подразделения или лицо его замещающее.

1.5. Ответственный за БИ осуществляет методическое руководство по обеспечению безопасности информации и контроль выполнения требований по обеспечению безопасности информации.

2. ФУНКЦИИ

Ответственный за БИ отвечает за:

2.1. Осуществление внутреннего контроля в структурном подразделении.

2.2. Соблюдение требований к защите информации.

2.3. Доведение до должностных лиц положений законодательства Российской Федерации, правовых актов по вопросам обработки информации, требований к защите информации с соответствующими записями в дневники индивидуально-воспитательной работы.

2.4. Осуществление контроля за обработкой информации.

2.5. Организацию контроля за соблюдением инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей по вопросам защиты информации.

2.6. Оценку эффективности применяемых мер по обеспечению безопасности информации.

2.7. Организует разработку и контроль за исполнением Плана мероприятий по защите информации в структурном подразделении.

3. ОБЯЗАННОСТИ

Ответственный за БИ обязан:

3.1. Проверять соблюдение правил доступа к информации.

3.2. Проверять порядок применения средств защиты информации.

3.3. Организовывать обработку и использование информации исключительно в целях, предусмотренных нормативными правовыми актами РФ.

3.4. Организовывать обеспечение безопасности информации требуемому уровню защищенности.

3.5. Осуществлять контроль содержания и объема обрабатываемых информации и соответствия их перечню.

3.6. Определять порядок и условия применения организационных и технических мер по обеспечению безопасности информации необходимых при обработке и выполнении требований к защите информации, исполнение которых обеспечивает установленные уровни защищенности информации.

3.7. Проводить анализ эффективности применения мер по обеспечению безопасности информации.

3.8. Контролировать состояние учета машинных носителей информации и носителей ключевой информации.

3.9. Контролировать проведение мероприятий восстановлению информации, модифицированных или уничтоженных вследствие несанкционированного доступа к ней.

3.10. Контролировать проведение мероприятий по резервированию информации.

3.11. Ознакомлять должностных лиц с положениями законодательства Российской Федерации с занесением соответствующих записей в журнал ознакомления.

3.12. Проводить мероприятия по защите информации согласно утверждённому плану.

3.13. Осуществлять контроль выполнения требований действующих нормативных документов по вопросам защиты информации.

3.14. Проводить занятия с пользователями по правилам работы на АРМ, оснащенных СЗИ, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

3.15. Участвовать в расследовании причин совершения нарушений безопасности информации.

4. ПРАВА

Ответственный за БИ имеет право:

4.1. Требовать от всех пользователей информационных систем выполнения установленных правил обработки информации, инструкций и других нормативных правовых документов по обеспечению безопасности информации.

4.2. Запрашивать у должностных лиц информацию, необходимую для реализации полномочий.

4.3. Участвовать в разработке мероприятий по совершенствованию безопасности информации.

4.4. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4.5. Осуществлять проверки по контролю соответствия обработки информации требованиям к защите информации.

4.6. Требовать от ответственных должностных лиц уточнения, блокирования или уничтожения недостоверной, или полученной незаконным путем информации.

4.7. Инициировать проведение расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов вычислительной техники.

4.8. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4.9. Применять меры по приостановлению или прекращению обработки информации, осуществляемой с нарушением требований законодательства Российской Федерации.

4.10. Вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации при их обработке.

5. ОТВЕТСТВЕННОСТЬ

Ответственный за БИ несёт ответственность в пределах, определённых действующими нормативными документами:

5.1. За ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящим должностным регламентом (должностной инструкцией).

5.2. За неправильность и неполноту использования предоставленных ему прав.

5.3. За правонарушения, совершенные в процессе осуществления своей деятельности.

5.4. За реализацию принятой политики информационной безопасности.

5.5. За разглашение сведений, конфиденциального характера, ставших известными ему по роду работы.

Заместитель начальника учебного центра Е.В.Шевченко

Приложение № 5
к приказу начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.21г № 54

ИНСТРУКЦИЯ ОТВЕТСТВЕННОМУ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПОСТРАНЕНИЯ ОБЪЕКТОВ ИНФОРМТИЗАЦИИИ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Должностная инструкция ответственному за организацию обработки и обеспечения информации ограниченного распространения объектов информатизации учебного центра (далее – Инструкция) определяет, обязанности и права лица, назначенного ответственным за организацию обработки и обеспечения безопасности информации ограниченного распространения объектов информатизации учебного центра (далее – ответственный за БИОР).

1.2. Инструкция разработана в соответствии с требованиями:

1.2.1. Трудового кодекса Российской Федерации;

1.2.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.2.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

1.2.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.2.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»

1.2.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «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»;

1.2.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.2.8. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.2.10. Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.3. Ответственный за БИОР назначается приказом начальника учебного центра.

1.4. Ответственный за БИОР в структурных подразделениях учебного центра назначается начальник структурного подразделения или лицо его замещающее.

1.5. Ответственный за БИОР осуществляет методическое руководство по обеспечению безопасности информации и контроль выполнения требований по обеспечению безопасности информации.

2. ФУНКЦИИ

Ответственный за БИОР отвечает за:

2.1. Осуществление внутреннего контроля в структурном подразделении;

2.2. Соблюдение требований к защите информации;

2.3. Доведение до должностных лиц положений законодательства Российской Федерации, правовых актов по вопросам обработки информации, требований к защите информации с соответствующими записями в дневники индивидуально-воспитательной работы;

2.4. Осуществление контроля за обработкой информации.

2.5. Организацию контроля за соблюдением инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей по вопросам защиты информации

2.6. Оценку эффективности применяемых мер по обеспечению безопасности информации.

2.7. Организует разработку и контроль за исполнением Плана мероприятий по защите информации в структурном подразделении.

3. ОБЯЗАННОСТИ

Ответственный за БИОР обязан:

3.1. Проверять соблюдение правил доступа к информации ограниченного распространения.

3.2. Проверять порядок применения средств защиты информации.

3.3. Организовывать обработку и использование информации ограниченного распространения исключительно в целях, предусмотренных нормативными правовыми актами РФ.

3.4. Организовывать обеспечение безопасности информации ограниченного распространения требуемому уровню защищенности.

3.5. Осуществлять контроль содержания и объема обрабатываемой информации.

3.6. Определять порядок и условия применения организационных и технических мер по обеспечению безопасности информации ограниченного распространения необходимых при обработке и выполнении требований к защите информации, исполнение которых обеспечивает установленные уровни защищенности информации.

3.7. Проводить анализ эффективности применения мер по обеспечению безопасности информации.

3.8. Контролировать состояние учета носителей конфиденциальной информации;

3.9. Контролировать проведение мероприятий по восстановлению информации ограниченного распространения, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

3.10. Контролировать проведение мероприятий по резервированию информации ограниченного распространения;

3.11. Ознакомлять должностных лиц с положениями законодательства Российской Федерации с занесением соответствующих записей в журнал ознакомления;

3.12. Проводить мероприятия по защите информации ограниченного распространения согласно утверждённому плану;

3.13. Осуществлять контроль выполнения требований действующих нормативных документов по вопросам защиты информации ограниченного распространения;

3.14. Проводить занятия с пользователями по правилам работы на АРМ, оснащенных СЗИ, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

3.15. Участвовать в расследовании причин совершения нарушений безопасности информации ограниченного распространения.

4. ПРАВА

Ответственный за БИОР имеет право:

4.1. Требовать от всех пользователей информационных систем выполнения установленных правил обработки информации ограниченного распространения, инструкций и других нормативных правовых документов по обеспечению безопасности информации ограниченного распространения.

4.2. Запрашивать у должностных лиц информацию, необходимую для реализации полномочий.

4.3. Участвовать в разработке мероприятий по совершенствованию безопасности информации ограниченного распространения.

4.4. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4.5. Осуществлять проверки по контролю соответствия обработки информации ограниченного распространения требованиям к защите информации;

4.6. Требовать от ответственных должностных лиц уточнения, блокирования или уничтожения недостоверной, или полученной незаконным путем информации ограниченного распространения;

4.7. Инициировать проведение расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов вычислительной техники.

4.8. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4.9. Применять меры по приостановлению или прекращению обработки информации, осуществляемой с нарушением требований законодательства Российской Федерации;

4.10. Вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации ограниченного распространения при ее обработке.

5. ОТВЕТСТВЕННОСТЬ

Ответственный за БИ несёт ответственность в пределах, определённых действующими нормативными документами:

5.1. За ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящим должностным регламентом (должностной инструкцией).

5.2. За неправильность и неполноту использования предоставленных ему прав.

5.3. За правонарушения, совершенные в процессе осуществления своей деятельности.

5.4. За реализацию принятой политики информационной безопасности.

5.5. За разглашение сведений, конфиденциального характера, ставших известными ему по роду работы.

Заместитель начальника учебного центра Е.В.Шевченко

Приложение № 6
к приказу начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.21г. № 51

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Должностная инструкция Администратору безопасности информации в учебном центре (далее – Инструкция) определяет обязанности, права, ограничения и ответственность лица, назначенного администратором безопасности информации в учебном центре (далее – Администратор БИ).

1.2. Инструкция разработана в соответствии с требованиями:

1.2.1. Трудового кодекса Российской Федерации;

1.2.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.2.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О информации»;

1.2.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.2.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

1.2.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О информации» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

1.2.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите информации при их обработке в информационных системах информации»;

1.2.8. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации»;

1.2.10. Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации с использованием средств криптографической защиты информации, необходимых для выполнения

установленных Правительством Российской Федерации требований к защите информации для каждого из уровней защищенности».

1.3. Администратор БИ назначается приказом начальника учебного центра.

2. ФУНКЦИИ

2.1. Администратор БИ отвечает за:

2.1.1. Сопровождение средств защиты информации (далее – СЗИ) (в том числе криптографических, шифровальных) от несанкционированного доступа и основных технических средств (далее – ОТС).

2.1.2. Организацию разграничения доступа.

2.1.3. Поддержание работоспособности автоматизированных рабочих мест (далее – АРМ).

2.1.4. Организацию порядка учета электронных носителей информацией и носителей ключевой информации.

2.1.5. Организацию порядка учета, хранения и обращения с документами.

2.1.6. Обеспечение резервного копирования и восстановления информации.

2.2. Администратор БИ присваивает пользователям идентификационные данные и права доступа и контролирует их соответствие. При этом должны выполняться следующие требования:

2.2.1. Администратор БИ разрабатывает политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;

2.2.2. Администратор БИ передает пользователю его персональный идентификатор и сообщает пользователю его пароль, соответствующий требованиям парольной политики;

2.2.3. Администратор БИ обеспечивает пересмотр и, при необходимости, корректировку учетных записей пользователей ежеквартально;

2.2.4. Администратор БИ обеспечивает уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач.

2.3. Администратор БИ разрабатывает и контролирует реализацию антивирусной политики, а именно:

2.3.1. Контролирует работоспособность средств антивирусной защиты;

2.3.2. Реагирует на появление любых сообщений средств антивирусной защиты;

2.3.3. Имеет право на проведение внеплановой проверки на присутствие вирусов;

2.3.4. Периодически обновляет антивирусные базы данных.

2.4. Администратор БИ производит резервное копирование и восстановление системного и прикладного програмного обеспечения, выполняяследующие требования:

2.4.1. Обязательное резервное копирование производится в случае обнаружения неисправностей в работе технических средств;

2.4.2. Допускается обоснованное внеплановое резервное копирование информации по инициативе администратора ИБ, если это не нарушает технологию обработки информации;

2.4.3. Резервные копии с системным и прикладным програмым обеспечением хранятся на съемных дисках у администратора безопасности;

2.4.4. В процессе и по мере устранения сбоев администратор ИБ производит восстановление информации и СЗИ;

2.4.5. Все операции по резервированию и восстановлению информации должны быть зарегистрированы.

3. ОБЯЗАННОСТИ

Администратор БИ обязан:

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации;

3.2. Знать перечень защищаемых информационных ресурсов;

3.3. Знать эксплуатационную и техническую документацию СЗИ и средст криптографической защиты информации;

3.4. Осуществлять установку, настройку и сопровождение программного обеспечения и СЗИ;

3.5. Участвовать в приемке нового программного обеспечения;

3.6. Производить необходимые настройки подсистемы управления доступом АС от НСД и сопровождать их в процессе эксплуатации, при этом реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т;д;);

3.7. Восстанавливать программную среду, программные средства и настройки механизмов защиты ОС при сбоях;

3.8. Организовать учет машинных носителей информации;

3.9. Осуществлять контроль работоспособности СЗИ;

3.10. Систематически проверять состояние используемых СЗИ, осуществлять выборочную проверку правильности их настройки;

3.11. Осуществлять поддержку функционирования (настройку и сопровождение) применяемых на АРМ специальных программных и программно-аппаратных СЗИ;

3.12. Осуществлять учет и контроль за активацией, блокированием, уничтожением, составом и полномочиями пользователей;

3.13. Осуществлять контроль за разделением полномочий пользователей;

3.14. Обеспечивать контроль за строгим выполнением требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт;

3.15. Требовать от пользователей стирания остаточной информации на несъёмных носителях информации установленным порядком;

3.16. Осуществлять контроль за обеспечением защиты информации при взаимодействии пользователей с информационными сетями связи общего пользования;

3.17. Участвовать в расследовании причин совершения нарушений безопасности информации;

3.18. Организовывать защиту технических средств;

3.19. Осуществлять контроль за исполнением правил и процедур антивирусной и парольной защит;

3.20. Вести журналы:

3.20.1. Учета нештатных ситуаций;

3.20.2. Резервирования информационных ресурсов, не относящихся к конфиденциальной информации;

3.20.3. Учета средств криптографической защиты информации,эксплуатационной и технической документации к ним, ключевых документов;

3.20.4. Учета паролей.

3.21. Реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем, СЗИ, системного и прикладного программного обеспечения;

3.22. Обеспечивать (осуществлять) смену и ввод пароля для разграничения доступа к информационным ресурсам пользователей с периодичностью не реже одного раза в квартал;

3.23. Сообщать обо всех неисправностях аппаратно-программных средств.

3.24. Немедленно ставить в известность ответственного за обеспечение безопасности информации обо всех неисправностях аппаратно-программных средств ГИС и ИСПД.

3.25. Немедленно сообщать ответственному за обеспечение безопасности информации об имевших место попытках НСД к информации и техническим средствам вычислительной техники, а также принимать необходимые меры по устранению нарушений:

3.25.1. Установить причины, по которым стал возможным НСД;

3.25.2. Установить личность нарушителя;

3.25.3. Установить последствия, к которым привел НСД;

3.25.4. Зафиксировать документально случай НСД с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

4. ПРАВА

Администратор БИ имеет право:

4.1. Получать доступ к программным и аппаратным средствам ГИС и ИСПД, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ГИС, ИСПД и АРМ пользователей.

4.2. Проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки информации;

4.3. Требовать от пользователей автомазированных систем, ГИС и ИСПД выполнения инструкций по обеспечению безопасности и защиты информации.

4.4. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов.

4.5. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности.

4.6. Вносить свои предложения по совершенствованию мер защиты.

4.7. Обращаться к ответственному за обеспечение безопасности информации с требованием прекращения работы в автомазированной системе, ГИС и ИСПД при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;

4.8. Требовать от пользователя изменения его пароля.

5. ОГРАНИЧЕНИЯ

Администратору БИ запрещается:

5.1. Использовать служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации.

5.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

5.3. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПД, предоставлять такую возможность другим пользователям.

5.4. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки;

5.5. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы, блокированию доступа, потере информации без предупреждения пользователей.

5.6. Нарушать правила эксплуатации оборудования.

5.7. Корректировать, удалять, подменять журналы.

6. ОТВЕТСТВЕННОСТЬ

Администратор БИ несет ответственность в пределах, определённых действующими нормативными документами:

6.1. За ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящим должностным регламентом (должностной инструкцией).

6.2. За неправильность и неполноту использования предоставленных ему прав.

6.3. За правонарушения, совершенные в процессе осуществления своей деятельности.

6.4. За реализацию принятой политики информационной безопасности.

6.5. За функционирование программно-технических и криптографических средств защиты информации, средств вычислительной техники, информационно-вычислительные комплексов, сети и испд обработки информации.

6.6. За разглашение сведений, конфиденциального характера, ставших известными ему по роду работы.

6.7. За качество и последствия проводимых им работ по контролю действий пользователей при работе.

Заместитель начальника учебного центра Е.В.Шевченко

Приложение № 7
к приказу Начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.24 № 39

ИНСТРУКЦИЯ АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Должностная инструкция Администратору безопасности информации ограниченного распространения объектов информатизации структурных подразделений учебного центра (далее – Инструкция) определяет обязанности, права, ограничения и ответственность лица, назначенного администратором безопасности информации ограниченного распространения объектов информатизации структурных подразделений учебного центра (далее – Администратор БИОР).

1.2. Инструкция разработана в соответствии с требованиями:

1.2.1. Трудового кодекса Российской Федерации;

1.2.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.2.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О информации»;

1.2.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.2.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»

1.2.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О информации» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

1.2.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите информации при их обработке в информационных системах информации»;

1.2.8. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации»;

1.2.10. Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите информации для каждого из уровней защищенности».

1.3. Администратор БИОР назначается приказом начальника учебного центра.

2. ФУНКЦИИ

2.1. Администратор БИОР отвечает за:

2.1.1. Сопровождение средств защиты информации (далее – СЗИ) (в том числе криптографических, шифровальных) от несанкционированного доступа и основных технических средств (далее – ОТС).

2.1.2. Организацию разграничения доступа.

2.1.3. Поддержание работоспособности автоматизированных рабочих мест (далее – АРМ).

2.1.4. Организацию порядка учета электронных носителей информацией и носителей ключевой информации.

2.1.5. Организацию порядка учета, хранения и обращения с документами.

2.1.6. Обеспечение резервного копирования и восстановления информации.

2.2. Администратор БИОР присваивает пользователям идентификационные данные и права доступа и контролирует их соответствие. При этом должны выполняться следующие требования:

2.2.1. Администратор БИОР разрабатывает политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;

2.2.2. Администратор БИОР передает пользователю его персональный идентификатор и сообщает пользователю его пароль, соответствующий требованиям парольной политики;

2.2.3. Администратор БИОР обеспечивает пересмотр и, при необходимости, корректировку учетных записей пользователей ежеквартально;

2.2.4. Администратор БИОР обеспечивает уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач.

2.3. Администратор БИОР разрабатывает и контролирует реализацию антивирусной политики, а именно:

2.3.1. Контролирует работоспособность средств антивирусной защиты;

2.3.2. Реагирует на появление любых сообщений средств антивирусной защиты;

2.3.3. Имеет право на проведение внеплановой проверки на присутствие вирусов;

2.3.4. Периодически обновляет антивирусные базы данных.

2.4. Администратор БИОР производит резервное копирование и восстановление системного и прикладного програмного обеспечения, выполняяследующие требования:

2.4.1. Обязательное резервное копирование производится в случае обнаружения неисправностей в работе технических средств;

2.4.2. Допускается обоснованное внеплановое резервное копирование информации по инициативе администратора БИОР , если это не нарушает технологию обработки информации;

2.4.3. Резервные копии с системным и прикладным програмым обеспечением хранятся на съемных дисках у администратора безопасности;

2.4.4. В процессе и по мере устранения сбоев администратор ИБ производит восстановление информации и СЗИ;

2.4.5. Все операции по резервированию и восстановлению информации должны быть зарегистрированы.

3. ОБЯЗАННОСТИ

Администратор БИОР обязан:

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации;

3.2. Знать перечень защищаемых информационных ресурсов;

3.3. Знать эксплуатационную и техническую документацию СЗИ и средст криптографической защиты информации;

3.4. Осуществлять установку, настройку и сопровождение программного обеспечения и СЗИ;

3.5. Участвовать в приемке нового программного обеспечения;

3.6. Производить необходимые настройки подсистемы управления доступом АС от НСД и сопровождать их в процессе эксплуатации, при этом реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т;д;);

3.7. Восстанавливать программную среду, программные средства и настройки механизмов защиты ОС при сбоях;

3.8. Организовать учет машинных носителей информации;

3.9. Осуществлять контроль работоспособности СЗИ;

3.10. Систематически проверять состояние используемых СЗИ, осуществлять выборочную проверку правильности их настройки;

3.11. Осуществлять поддержку функционирования (настройку и сопровождение) применяемых на АРМ специальных программных и программно-аппаратных СЗИ;

3.12. Осуществлять учет и контроль за активацией, блокированием, уничтожением, составом и полномочиями пользователей;

3.13. Осуществлять контроль за разделением полномочий пользователей;

3.14. Обеспечивать контроль за строгим выполнением требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт;

3.15. Требовать от пользователей стирания остаточной информации на несъёмных носителях информации установленным порядком;

3.16. Осуществлять контроль за обеспечением защиты информации при взаимодействии пользователей с информационными сетями связи общего пользования;

3.17. Участвовать в расследовании причин совершения нарушений безопасности информации;

3.18. Организовывать защиту технических средств;

3.19. Осуществлять контроль за исполнением правил и процедур антивирусной и парольной защит;

3.20. Вести журналы:

3.20.1. Учета нештатных ситуаций;

3.20.2. Резервирования информационных ресурсов, не относящихся к конфиденциальной информации;

3.20.3. Учета средств криптографической защиты информации,эксплуатационной и технической документации к ним, ключевых документов;

3.20.4. Учета паролей.

3.21. Реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем, СЗИ, системного и прикладного программного обеспечения;

3.22. Обеспечивать (осуществлять) смену и ввод пароля для разграничения доступа к информационным ресурсам пользователей с периодичностью не реже одного раза в квартал;

3.23. Сообщать обо всех неисправностях аппаратно-программных средств.

3.24. Немедленно ставить в известность ответственного за обеспечение безопасности информации обо всех неисправностях аппаратно-программных средств ГИС и ИСПД.

3.25. Немедленно сообщать ответственному за обеспечение безопасности информации об имевших место попытках НСД к информации и техническим средствам вычислительной техники, а также принимать необходимые меры по устранению нарушений:

3.25.1. Установить причины, по которым стал возможным НСД;

3.25.2. Установить личность нарушителя;

3.25.3. Установить последствия, к которым привел НСД;

3.25.4. Зафиксировать документально случай НСД с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

4. ПРАВА

Администратор БИОР имеет право:

4.1. Получать доступ к программным и аппаратным средствам ГИС и ИСПД, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ГИС, ИСПД и АРМ пользователей.

4.2. Проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки информации;

4.3. Требовать от пользователей автомазированных систем, ГИС и ИСПД выполнения инструкций по обеспечению безопасности и защиты информации.

4.4. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов.

4.5. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности.

4.6. Вносить свои предложения по совершенствованию мер защиты.

4.7. Обращаться к ответственному за обеспечение безопасности информации с требованием прекращения работы в автомазированной системе, ГИС и ИСПД при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;

4.8. Требовать от пользователя изменения его пароля.

5. ОГРАНИЧЕНИЯ

Администратору БИОР запрещается:

5.1. Использовать служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации.

5.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

5.3. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПД, предоставлять такую возможность другим пользователям.

5.4. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки;

5.5. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы, блокированию доступа, потере информации без предупреждения пользователей.

5.6. Нарушать правила эксплуатации оборудования.

5.7. Корректировать, удалять, подменять журналы.

6. ОТВЕТСТВЕННОСТЬ

Администратор БИОР несет ответственность в пределах, определённых действующими нормативными документами:

6.1. За ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящим должностным регламентом (должностной инструкцией).

6.2. За неправильность и неполноту использования предоставленных ему прав.

6.3. За правонарушения, совершенные в процессе осуществления своей деятельности.

6.4. За реализацию принятой политики информационной безопасности.

6.5. За функционирование программно-технических и криптографических средств защиты информации, средств вычислительной техники, информационно-вычислительные комплексов, сети и испд обработки информации.

6.6. За разглашение сведений, конфиденциального характера, ставших известными ему по роду работы.

6.7. За качество и последствия проводимых им работ по контролю действий пользователей при работе.

Заместитель начальника учебного центра  Е.В.Шевченко

Приложение № 8
к приказу Начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.22г № 58

ИНСТРУКЦИЯ
ПО ПОРЯДКУ ИСПОЛЬЗОВАНИЯ, УЧЕТА И ХРАНЕНИЯ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по порядку использования, учета и хранения носителей информации в учебном центре (далее – Инструкция) определяет типы носителей информации, назначение, правила использования, порядок учета и хранения носителей информации, предоставляемых учебным центром для использования в повседневной и учебной деятельности, а также в автоматизированных системах (далее – АС), государственных информационных системах (далее – ГИС) и информационных системах персональных данных (далее – ИСПД).

1.2. Настоящая Инструкция разработана в соответствии с требованиями:

1.2.1. Трудового кодекса Российской Федерации;

1.2.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.2.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

1.2.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.2.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

1.2.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «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»;

1.2.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.2.8. Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.2.9. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.2.10. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.2.11. Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.3. Действие Инструкции распространяется на всех должностных лиц учебного центра.

1.4. Под использованием носителей информации в ГИС и ИСПД понимается их подключение к инфраструктуре с целью обработки, приема/передачи информации между АС, ГИС и ИСПД и носителями информации.

1.5. Носители информации предоставляются должностным лицам учебного центра по инициативе начальников структурных подразделений в случаях:

1.5.1. Необходимости выполнения вновь принятым должностным лицом своих должностных обязанностей;

1.5.2. Возникновения у должностного лица учебного центра служебной необходимости.

2. КЛАССИФИКАЦИЯ

2.1. Под носителей информации понимается физический объект, свойства и характеристики которого используются для записи и хранения данных.

2.2. В учебном центре выделяют следующие электронные носители информации:

2.2.1. Несъемные носители информации;

2.2.2. Съемные носители информации;

2.2.3. Носители ключевой информации.

2.3. К несъемным носителям информации относятся накопители на жестких магнитных дисках (жесткие диски или HDD) и устройства на основе flash-памяти (твердотельные накопители или SSD) установленные в корпусе системного блока автоматизированного рабочего места (далее – АРМ), демонтаж которых невозможен без доступа во внутреннее пространство АРМ.

2.4. К съемным носителям информации относятся устройства на основе flash-памяти и оптические диски (CD-ROM, DVD-ROM) установка и извлечение которых производится через специальные разъемы и устройства АРМ и без необходимости доступа во внутреннее пространство АРМ.

2.5. К носителям ключевой информации относятся устройства на основе flash-памяти, предназначенные для осуществления криптографической защиты информации в течение определенного срока.

3. ПРАВИЛА ИСПОЛЬЗОВАНИЯ

3.1. Под использованием носителей понимается их подключение к инфраструктуре информационной системы с целью обработки, приема и (или) передачи информации между информационными системами и носителем.

3.2. При использовании должностными лицами носителей информации обязаны:

3.2.1. Соблюдать требования настоящей Инструкции;

3.2.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей;

3.2.3. Ставить в известность ответственных должностных лиц о любых фактах нарушения требований настоящей Инструкции;

3.2.4. Бережно относится к носителям информации;

3.2.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами;

3.2.6. Извещать ответственных о фактах утраты (кражи) носителей персональных данных;

3.3. При использовании носителей информации должностным лицам запрещается;

3.3.1. Использовать носители в личных целях;

3.3.2. Передавать носители другим лицам (за исключением ответственных должностных лиц);

3.3.3. Хранить съемные носители с конфиденциальной информацией вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

3.3.4. Выносить съемные носители с конфиденциальной информацией из служебных помещений для работы с ними на дому и т. д;

3.3.5. Любое действие (обработка, прием/передача информации) инициированное должностным лицом с использованием неучтенных (личных) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с ответственным должностным лицом заранее).

3.4. Ответственные должностные лица оставляют за собой право блокировать или ограничивать использование носителей информации.

3.5. Информация об использовании должностными лицами носителей информации протоколируется и, при необходимости, может быть предоставлена начальникам структурных подразделений.

3.6. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициализируется служебное расследование.

3.7. При отправке или передаче конфиденциальной информации адресатам на носители информации записываются только предназначенные адресатам данные.

3.8. Съемные носители информации с конфиденциальной информацией, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

3.9. В случае утраты или уничтожения съемных носителей информации с конфиденциальной информацией либо разглашении содержащихся в них сведений

немедленно ставится в известность начальник структурного подразделения и ответственное должностное лицо.

3.10. В случае увольнения или перевода должностного лица в другое структурное подразделение, предоставленные носители информации изымаются.

3.11. Информация, хранящаяся на носителях информации, подлежит обязательной проверке на отсутствие вредоносного программного заражения.

4. УЧЕТ И ХРАНЕНИЕ

4.1. Все находящиеся в обращении и на хранении носители информации подлежат учёту.

4.2. Каждый носитель информации должен иметь бирку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу носителей информации осуществляют должностные лица структурных подразделений, на которых возложены функции их хранения и учета.

4.4. В Журналах учета носителей учитываются несъемные и съемные носителям информации в том числе на которых находиться конфиденциальная информация.

4.5. В Журнале учета носителей ключевой информации учитываются носители ключевой информации.

4.6. В журналах учета указывается как уникальный учетный номер, так и «GUID класса» носителя информации.

4.7. Уникальный учётный номер носителя состоит из:

4.7.1. Сокращенного наименования структурного подразделения;

4.7.2. Разделителя в виде тире «-»;

4.7.3. Порядкового номера по журналу;

4.7.4. Разделителя в виде наклонного тире «/»;

4.7.5. Типа носителя.

4.8. Носители информации разделяются и обозначаются:

4.8.1. «Н» для несъемных носителей;

4.8.2. «С» для съемных носителей

4.8.3. «К» для ключевых носителей

4.9. Пример уникального учётного номера носителя - №УО-01/Н, где «УО» – учебный отдел, «01» – порядковый номер в журнале, «Н» – несъемный носитель информации.

4.10. В случае отсутствия утвержденных сокращений названий подразделений учетный номер носителя состоит из:

4.10.1. Порядкового номера по журналу;

4.10.2. Разделителя в виде наклонного тире «/»

4.10.3. Типа носителя.

4.11. Пример уникального учётного номера носителя без утвержденного сокращения подразделения - №01/С, где «01» – порядковый номер в журнале, «С» - съемный носитель информации.

4.12. Для съемных носителей информации реквизиты наносятся непосредственно на носитель (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяется маркировка упаковки, в которой хранится носитель или другие доступные способы маркировки (бирки, брелоки и т.п.).

4.13. Надпись реквизитов делается разборчиво и аккуратно, также допускается наклеивать заранее заготовленную этикетку.

4.14. Должностные лица получают учтенный носитель информации от ответственного должностного лица для выполнения работ на конкретный срок с соответствующей записью в журнале учета.

4.15. По окончании работ должностное лицо сдает носитель уполномоченному должностному, о чем делается соответствующая запись в журнале учета.

4.16. Вынос съемных носителей информации с конфиденциальной информацией для непосредственной передачи адресату осуществляется только с письменного разрешения начальника структурного подразделения.

4.17. На утраченные и уничтоженные носители информации составляются акты, в которых содержатся процедуры уничтожения и делаются соответствующие отметки в журналах учета.

5. ОТВЕТСТВЕННОСТЬ

5.1. Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации и локальными нормативными актами.

Заместитель начальника учебного центра Е.В.Шевченко

Приложение № 9
к приказу начальника ФАУ ДПО
Краснодарский учебный центр ФПС
от 15.02.24г. № 51

ИНСТРУКЦИЯ ПО ПОРЯДКУ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ И АНТИВИРУСНОЙ ЗАЩИТЫ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по порядку организации парольной и антивирусной защит в учебном центре (далее – Инструкция) определяет порядок организации парольной и антивирусной защиты в учебном центре, в том числе в автоматизированных системах (далее – АС) государственных информационных системах (далее – ГИС) и информационных системах персональных данных (далее – ИСПД).

1.2. Настоящая Инструкция предназначена для уполномоченных должностных лиц учебного центра в том числе:

1.2.1. Ответственного за обеспечение требований по технической защите информации учебного центра;

1.2.2. Ответственных за методическое руководство и контроль за эффективностью предусмотренных мер защиты информации;

1.2.3. Ответственных за организацию обработки и обеспечение безопасности информации структурных подразделений учебного центра;

1.2.4. Ответственных за организацию обработки и обеспечения безопасности персональных данных объектов информатизации (далее – ОИ) структурных подразделений учебного центра;

1.2.5. Ответственных за организацию обработки и обеспечения безопасности информации ограниченного распространения ОИ структурных подразделений учебного центра;

1.2.6. Администратора безопасности информации (далее - Администратор БИ) ОИ структурных подразделений учебного центра;

1.2.7. Администратора безопасности персональных данных (далее - Администратор БПН) ОИ структурных подразделений ГУ МЧС России по Краснодарскому краю;

1.2.8. Администратора безопасности информации ограниченного распространения (далее - Администратор БИОР) ОИ структурных подразделений учебного центра;

1.2.9. Пользователей информационных и автоматизированных систем.

1.3. Действие Инструкции распространяется на структурные подразделения учебного центра.

1.4. Инструкция разработана в соответствии с требованиями:

1.4.1. Трудового кодекса Российской Федерации;

1.4.2. Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

1.4.3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

1.4.4. Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

1.4.5. Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»

1.4.6. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «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»;

1.4.7. Постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.4.8. Приказа ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.4.9. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.4.10. Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.5. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей и контроль за действиями пользователями при работе с паролями во всех АС, ГИС и ИСПД возлагается на администраторов безопасности.

1.6. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ, внешних нарушителей на всех автоматизированных рабочих местах учебного центра должна быть организована:

1.6.1. Парольная защита;

1.6.2. Антивирусная защита;

1.7. Антивирусные средства защиты должны быть лицензионными и иметь сертификат соответствия требованиям безопасности, выданный Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК) России.

1.8. Рабочие места рекомендуется оснащать одним антивирусным программным обеспечением.

1.9. Параметры антивирусной политики задаются ответственным за организацию обработки и обеспечения безопасности информации.

1.10. Реализация параметров антивирусной политики осуществляется администраторами безопасности.

1.11. Антивирусные средства защиты должны функционировать исправно и непрерывно.

1.12. При сбоях в работе требуется немедленное вмешательство администратора безопасности для устранения неполадок.

2. ПРАВИЛА СОЗДАНИЯ ПАРОЛЯ

2.1. Длина пароля должен быть не менее 10 символов.

2.2. Пароль может состоять из:

2.2.1. Прописных букв английского алфавита (от A до Z);

2.2.2. Строчных букв английского алфавита (от a до z);

2.2.3. Десятичных цифр (от 0 до 9);

2.2.4. Символов, не принадлежащих алфавитно-цифровому набору (например, !, $, #, %).

2.3. Пароль должен состоять как минимум из трёх категорий вышеперечисленных символов.

2.4. Пароль не должен содержать:

2.4.1. Имя учетной записи пользователя или какую-либо его часть;

2.4.2. Имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

2.4.3. Комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

2.4.4. Комбинации символов, которые уже использовались ранее.

2.5. Запрещается использовать в качестве пароля:

2.5.1. Имя входа в систему;

2.5.2. Простые пароли типа «123», «111», «qwerty» и им подобные;

2.5.3. Один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1. Бесконтрольность в определении и использовании паролей в информационных и автоматизированных системах учебного центра может повлечь:

3.1.1. Несанкционированный доступ к информации;

3.1.2. Мошеннические воздействия;

3.1.3. Деструктивных воздействия.

3.2. Первоначальные пароли выдаются пользователям Администраторами безопасности.

3.3. Минимальное время смены пароля - 1 день.

3.4. Максимальное время смены пароля – 90 дней.

3.5. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

3.6. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами.

3.7. Хранение паролей на бумажных носителях должно осуществляться только в запираемых сейфах или других труднодоступных местах.

3.8. Хранение паролей в электронном виде должно осуществляться на съемных носителях информации в зашифрованном виде.

3.9. Запрещается хранение съемных носителей с паролями в доступных местах.

3.10. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.11. Лица, использующие пароли, обязаны:

3.11.1. Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

3.11.2. Своевременно сообщать об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей ответственным за организацию обработки и обеспечения безопасности и администраторам безопасности.

4. КОМПРОМЕТАЦИЯ ПАРОЛЕЙ

4.1. Пользователь при компрометации или подозрении на компрометацию своего пароля, утере личного идентификатора обязан без промедления сообщить об этом администратору безопасности.

4.2. Администратор безопасности должен провести следующие мероприятия:

4.2.1. Взять объяснительную в письменном виде с пользователя, обнаружившего компрометацию пароля.

4.2.2. Объяснительная пишется на имя начальника учебного центра и должна содержать ФИО, должность пользователя, описание обстоятельств, при которых была обнаружена компрометация, утеря личного идентификатора или описание причин подозрения на компрометацию, последние действия, проведенные в автоматизированной системе, личную подпись пользователя;

4.2.3. Произвести внеочередную смену пароля пользователя или, при утере личного идентификатора, блокировку учетной записи пользователя, для предотвращения использования третьими лицами данной учетной записи;

4.2.4. В случае выявления действий, не указанных пользователем в объяснительной, проводится служебное расследование по выяснению причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины нанесенного ущерба безопасности информации;

4.2.5. В случае не обнаружения никаких признаков использования пароля или идентификатора пользователя в несанкционированных целях, составляется акт об отсутствии нарушений при использовании пароля.

5. ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

5.1. Основными параметрами антивирусной защиты являются:

5.1.1. Периодичность обновления антивирусных баз;

5.1.2. Периодичность проверки наличия/отсутствия вирусных заражений;

5.1.3. Параметры проверки «на лету» при работе в сети передачи данных «Интернет» (далее – СПД «Интернет»).

5.2. Обязательной антивирусной защите подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях.

5.3. Основными задачами антивирусной защиты являются:

5.3.1. Исключение или существенное затруднение противоправных действий в отношении носителей защищаемой информации;

5.3.2. Обеспечение условий для устойчивой бесперебойной работы объектов, сетей передачи данных.

5.4. Объектом защиты от воздействия вредоносных программ являются вычислительные структуры и транспортная среда передачи данных.

5.5. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на администраторов безопасности структурного подразделения.

5.6. Периодический контроль состояния антивирусной защиты возлагается на администраторов безопасности структурного подразделения.

5.7. Должностные лица, на которых возлагается ответственность по антивирусной защите, имеют полноправный доступ ко всем рабочим станциям, серверам и другому оборудованию АС, ГИС и ИСПД.

5.8. Все процессы производятся в автоматическом режиме без участия пользователей и без помех для работы основного и специального программного обеспечения.

5.9. В основные обязанности по антивирусной защите входит:

5.9.1. Проведение периодического анализа и оценки ситуации по обеспечению антивирусной безопасности для контроля степени защищенности и выработки предложений по изменению и улучшению состояния дел;

5.9.2. Проверка соблюдения порядка обновления средств и баз данных антивирусной защиты;

5.9.3. Осуществление контроля за состоянием средств антивирусной защиты на серверах, рабочих станциях;

5.9.4. Осуществление контроля за соблюдением требований по обеспечению антивирусной защиты;

5.9.5. Передача ежеквартального отчета по состоянию антивирусной защиты ответственному за организацию обработки и обеспечение безопасности.

5.10. Ответственный за организацию обработки и обеспечение безопасности осуществляют следующие действия:

5.10.1. Контроль и анализ отчетов по состоянию антивирусной защиты;

5.10.2. Организацию проведения служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) разрушение технологического оборудования, локально-вычислительной сети и информационных массивов;

5.10.3. Организацию мероприятий по улучшению антивирусной защиты.

5.11. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вредоносных программ.

5.12. Непосредственно после установки (изменения) программного обеспечения, администратор безопасности либо уполномоченное должностные лицо подразделения выполняет антивирусную проверку.

5.13. При возникновении подозрения на наличие вредоносных программ администратор безопасности либо уполномоченное должностные лицо подразделения проводит внеочередной антивирусный контроль.

5.14. Для пользователей рабочих станций запрещена возможность изменения настроек и параметров защиты антивирусных средств на своей рабочей станции, эти действия производит администратор безопасности или уполномоченное должностные лицо подразделения с помощью средств централизованного управления или вручную.

5.15. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя технологического оборудования, локально-вычислительной сети и информационных массивов, проводится служебное расследование.

5.16. Результаты расследования причин появления и последствий воздействия вредоносных программ на рабочую станцию (сервер) докладываются ответственному за обеспечение требований по технической защите информации ГУ МЧС России по Краснодарскому краю с предложениями по принятию мер, предотвращающих в будущем повторение подобных фактов.

6. ПОРЯДОК РАБОТЫ СО СРЕДСТВАМИ АНТИВИРУСНОЙ ЗАЩИТЫ

6.1. На каждое автоматизированное рабочее место администратором безопасности устанавливается и настраивается антивирусное средство защиты.

6.2. Пользователь автоматизированного рабочего места не должен препятствовать обновлению антивирусных баз или проверке наличия/отсутствия вирусных заражений, а также реагировать на предупреждения антивирусного средства защиты при работе в сети СПД «Интернет».

6.3. Пользователь при работе со съемными носителями информации должен перед использованием носителя проверить его на наличие вирусов или вредоносного программного обеспечения.

6.4. Администратор безопасности при обращении к нему пользователей с зараженными носителями информации должен еще раз проверить носитель, выяснить причину невозможности «вылечить» зараженный файл и по возможности удалить этот файл.

6.5. При подозрении на вирусное заражение автоматизированного рабочего места, пользователь должен незамедлительно сообщить об этом администратору безопасности.

6.6. Признаками вирусного заражения являются:

6.6.1. Работоспособность компьютера значительно снижается;

6.6.2. Появляются различного рода диалоговые окна интернет-характера;

6.6.3. Самопроизвольно открываются/закрываются используемые в работе проводниковые окна, файлы, программы;

6.6.4. Появление на экране монитора баннера.

Заместитель начальника учебного центра Е.В. Шевченко

Приложение № 10
к приказу Начальника ФАУ ДПО
Краснодарский учебный центр
ФПС
от_____ № _____

ФОРМЫ ЖУРНАЛОВ, ИСПОЛЬЗУЮЩИХСЯ ПРИ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТ В ФАУ ДПО КРАСНОДАРСКИЙ УЧЕБНЫЙ ЦЕНТР ФПС

1. ФОРМА ЖУРНАЛА УЧЕТА СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, НЕ ОТНОСЯЩЕЙСЯ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1.1. Сторона «А»:

№ п/п	Носитель информации					Отметка о выдачи носителя	
	Дата регистрации	Регистрационный номер	«GUID класса» носителя	Тип/ёмкость носителя (FLASH-карта/CD-R/CD-RW/DWD-R/DWD-RW диск, ГБ.)	Назначение носителя информации (хранение/резервирование/передача)	Ф.И.О. получившего носитель	Дата выд и подпи получивш носител
1.	2.	3.	4.	5.	6.	7.	8.

1.2. Сторона «Б»:

Отметка о получении носителя				Отметка о сдачи носителя		Отметка об убытии носителя		Сведени уничтож носите (причи ФИО подпис дата)
Дата и номер сопроводи-тельного документа о передачи носителя	От кого получен носитель	Ф.И.О. ответственного за носитель	Дата получения и подпись ответственного за носитель	Дата сдачи носителя	подпись ответственного за носитель	Куда убыл носитель	Дата и номер сопроводи-тельного документа о передачи носителя	
9.	10.	11.	12.	13.	14.	15.	16.	17.

2. ФОРМА ЖУРНАЛА УЧЕТА НОСИТЕЛЕЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ

2.1. Сторона «А»:

№ п/п	Носитель информации					Отметка о выдачи носителя	
	Дата регистрации	Регистрационный номер	«GUID класса» носителя	Тип носителя/АС, ГИС ИСПД для которой предназначен носитель. (ru-token, e-token,)	Тип хранимой информации (сертификат, закрытый ключ, открытый ключ, и д.р)	Ф.И.О. получившего носитель	Дата выда и подпи получивш носител
1.	2.	3.	4.	5.	6.	7.	8.

2.2. Сторона «Б»:

Отметка о получении носителя				Отметка о сдачи носителя		Отметка об убытии носителя		Сведени уничтож носите (причи ФИО подпис дата)
Дата и номер сопроводи-тельного письма, Распоряжения, Приказа о передачи носителя	От кого получен носитель	Ф.И.О. ответственного за носитель	Дата получения и подпись ответственного за носитель	Дата сдачи носителя	подпись ответственного за носитель	Куда убыл носитель	Дата и номер сопроводи-тельного письма, Распоряжения, Приказа о передачи носителя	
9.	10.	11.	12.	13.	14.	15.	16.	17.

3. ФОРМА ЖУРНАЛА УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ

№ п/п	Дата и время	АРМ (сервер, ресурс сети, учетная запись) на котором зафиксирована нештатная ситуация	Описание нештатной ситуации (коме зафиксирована, тип нештатной ситуации и д.р.)	Принятые меры, Проинформированные лица (ФИО, должность), дата и время (ДД.ММ.ГГГГ, ЧЧ:ММ) информирования	Отметка о ликвидации нештатной ситуация (ФИО подпись ответственн
1.	2.	3.	4.	5.	6.

4. ФОРМА ЖУРНАЛА РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ, НЕ ОТНОСЯЩИХСЯ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

№ п/п	Дата	Вид резервирования (полное/частичное)	Резервируемый ресурс (файлы/ папки/ базы данных/ и тд.)	Объем архива, (МБ)	Регистрационный номер носителя информации	Ответственн лицо произвед резервирован (ФИО, подпи
1.	2.	3.	4.	5.	6.	7.

5. ФОРМА ЖУРНАЛА УЧЕТА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

5.1. Сторона «А»:

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации, ключевых документов	Регистрационный (серийный, инвентарный) номер СКЗИ, эксплуатационной и технической документации, ключевых документов	Отметка о получении				Отметка о выдачи		Отметка о установке		
			От кого получены (должностное лицо /организация)	Дата и номер сопроводи - тельного письма, Распоряжения, Приказа о передачи	Ф.И.О. ответственного	Дата получения и подпись ответственного	Ф.И.О. пользователя СКЗИ	Дата выдачи и подпись пользователя	Ф.И.О. ответственного, производившего установку	Дата установки и подпись лица, произведшего установку	Ном аппар ы сред в кото устан ен СК
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	1

5.2. Сторона «Б»:

Отметка об изъятии СКЗИ из аппаратных средств			Отметка о сдачи		Отметка об убытии	
Дата изъятия (уничтожения)	Ф.И.О. ответственного производившего изъятие (уничтожение)	подпись ответственного, произведшего изъятие (№ акта уничтожения)	Дата сдачи СКЗИ	Подпись ответственного	Куда убыло	Дата и номер сопроводительно письма, Распоряжения Приказа о переда
13.	14.	15.	16.	17.	18.	19.

6. ФОРМА ЖУРНАЛА УЧЕТА ПАРОЛЕЙ

№ п/п	ФИО Пользователя	Наименование системы	Логин	Пароль	Дата выдачи	ФИО выдавшего пароль	Подпись выдавшего	Подпись получивш
1.								
2.								
3.								

Заместитель начальника учебного центра **Е.В.Шевче**