УТВЕРЖДЕН
приказом Государственного учреждения
социального обслуживания «Хохотуйский
центр помощи детям, оставшимся без
попечения родителей «Берёзка»
Забайкальского края
от «7» июня 2023 года № 784

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах Государственного учреждения социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края

с. Хохотуй
2024

I. Назначение

1.1. Настоящая Инструкция по организации антивирусной защиты в информационных системах Государственного учреждения социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края (далее – Инструкция, Учреждение соответственно) определяет требования к организации защиты информационных систем от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителя Учреждения, ответственного за организацию обеспечения безопасности информации в информационных системах Учреждения, администратора безопасности информации, системных администраторов и пользователей за выполнение данных требований.

II. Область применения

2.1. Настоящая Инструкция применяется администратором безопасности информации, системным администратором и пользователями любых информационных систем, используемых в работе Учреждения.

III. Нормативные ссылки

3.1. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01.11.2012 № 1119;
- Требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными Постановлением Правительства РФ от 06.07.2015 № 676;
- Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17 (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- Составом и содержанием 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, утвержденными приказом ФСБ России от 10.07.2014 № 378 (зарегистрировано в Минюсте России 18.08.2014 № 33620);
- Специальными требованиями и рекомендациями по технической защите

конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282;

- Методическим документом «Меры защиты информации в государственных информационных системах» (утверждено ФСТЭК России 11.02.2014);

- ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство;

- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

IV. Термины, обозначения и сокращения

4.1. В настоящей Инструкции используются следующие термины и определения:

4.1.1. **Автоматизированная система (АС)** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

4.1.2. **Администратор безопасности информации** - лицо, отвечающее за защиту автоматизированных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации.

4.1.3. **Аппаратно-программные методы защиты** ПС от КВ реализуются с помощью специализированного устройства - контроллера, вставляемого в один из разъемов расширения компьютера, и специального программного обеспечения, управляющего работой этого контроллера и реализующего один или несколько из программных методов.

4.1.4. **Безопасность информации [данных]** - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

4.1.5. **Вакцинирование** - обработка файлов, дисков, каталогов, проводимая с применением специальных программ, создающих условия, подобные тем, которые создаются определенным компьютерным вирусом, и затрудняющих повторное его появление.

4.1.6. **Вредоносная программа** - программа, используемая для несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

4.1.7. **Информационная система (ИС)** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных

технологий и технических средств.

4.1.8. **Информационная система персональных данных (ИСПДн)**- совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4.1.9. **Компьютерный вирус (КВ)** - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

4.1.10. **Метод вакцинирования** устанавливает способ защиты любой конкретной программы от КВ, при котором к этой программе присоединяется специальный модуль контроля, следящий за ее целостностью. При этом проверяются контрольная сумма программы или какие-либо другие ее характеристики. Если КВ заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

4.1.11. **Метод обнаружения изменений** заключается в том, что антивирусная программа предварительно запоминает характеристики всех областей диска, которые могут подвергаться нападению КВ, а затем периодически проверяет их. Если изменение этих характеристик будет обнаружено, то такая программа сообщит пользователю, что, возможно, в компьютер попал КВ.

4.1.12. **Метод сканирования** заключается в том, что специальная антивирусная программа, называемая сканером, последовательно просматривает проверяемые файлы в поиске так называемых "сигнатур" известных КВ.

4.1.13. **Метод резидентных сторожей** использует антивирусные программы, которые постоянно находятся в оперативной памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Резидентный сторож сообщит пользователю о том, что какая-либо программа пытается изменить загрузочный сектор жесткого диска или дискеты, а также выполнимый файл.

4.1.14. **Метод эвристического анализа** реализуется с помощью антивирусных программ, которые проверяют остальные программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для КВ. Так, например, эвристический анализатор может обнаружить, что в проверяемой программе присутствует код, устанавливающий резидентный модуль в памяти.

4.1.15. **Пользователь (потребитель) информации** – 1) субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею; 2) работник Министерства, допущенный в установленном порядке к работе с конфиденциальной информацией, полномочия которого регламентированы внутренними организационно- распорядительными актами.

4.1.16. **Ревизоры**- антивирусные программы, основанные на обнаружении

изменений программной среды.

4.1.17. **Сигнатура** - уникальная последовательность байтов, принадлежащая конкретному известному КВ и не встречающаяся в других программах.

4.1.18. **Система защиты информации информационных систем (СЗИИС)** – 1) система по обеспечению безопасности защищаемой информации, создаваемая в соответствии с нормативными правовыми актами с целью нейтрализации актуальных угроз безопасности защищаемой информации; 2) система защиты информации информационных систем включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации и информационных технологий, используемых в информационных системах.

4.1.19. **Съемные машинные носители информации (СМНИ)** - физические устройства (дискеты, e-Token, смарт-карты и т.д.), предназначенные для хранения информации в электронной форме.

4.1.20. **Целостность информации** – 1) Устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации. Состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.

4.1.21. **Удаленный доступ** (remote access)- процесс получения доступа к сетевым ресурсам из другой сети или с терминала, не являющегося постоянно соединенным физически или логически с сетью, к которой он получает доступ.

4.1.22**. Удаленный пользователь** (remote user)- пользователь, находящийся на объекте (площадке, филиале), отличном от того, на котором размещаются используемые сетевые ресурсы.

4.2. В настоящей Инструкции используются следующие сокращения:

4.2.1. **АС** – автоматизированная система;

4.2.2. **ГИС-** государственная информационная система (в тексте настоящей Инструкции под ГИС понимаются ГИС «ППО АИСТ ГБД» и ГИС «АС «АСП»);

4.2.3. **ИСПДн** - информационная система персональных данных;

4.2.4. **КВ** – компьютерный вирус;

4.2.5. **ПДн** – персональные данные;

4.2.6. **ПО** – программное обеспечение;

4.2.7. **ПС** - программные средства;

4.2.8. **ПЭВМ** – персональная электронно - вычислительная машина;

4.2.9. **СЗИИС** – система защиты информации информационных систем;

4.2.10. **СМНИ** - съемные машинные носители информации.

V. Общие положения

5.1. К использованию при работе в информационных системах Учреждения допускаются только сертифицированные антивирусные средства, закупленные у

разработчиков (или официальных поставщиков) указанных средств.

5.2. При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

5.3. Установка средств антивирусного контроля в ИС осуществляется администратором безопасности информации (программистом) в соответствии с руководствами по применению конкретных антивирусных средств.

5.4. Контроль состояния и реализация антивирусной защиты информационных систем Учреждения возлагается на администратора безопасности информации (программиста).

5.5. Сотрудники Учреждения, допущенные к работе с защищаемой информацией в ИС, обязаны уметь пользоваться средствами антивирусной защиты.

5.6. Сотрудникам Учреждения запрещено самовольное отключение средств антивирусной защиты.

5.7. Пользователи должны срочно поставить в известность администратора безопасности информации (программиста), в случае обнаружения попыток несанкционированного доступа в систему, при обнаружении вирусной атаки системы, а также в других случаях, связанных с информационной безопасностью. Администратор безопасности информации (программист) обязан регулярно докладывать руководителю Учреждения служебной запиской о результатах периодической проверки состояния антивирусной защиты информационных систем.

VI. Реализация антивирусной защиты

6.1. В информационных системах должны выполняться следующие требования Регуляторов к реализации антивирусной защиты:

6.1.1. Администратором безопасности информации (программистом) должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

6.1.2. Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках

доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);

- установку, конфигурирование и управление средствами антивирусной защиты;

- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

- оповещение администратора безопасности (программиста) в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

6.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по реализации антивирусной защиты:

6.2.1. В информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности (программисту).

6.2.2. В информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах).

6.2.3. В Учреждении должен обеспечиваться запрет использования съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (вирусов).

6.2.4. В информационной системе должно обеспечиваться использование на разных уровнях информационной системы средств антивирусной защиты разных производителей.

6.2.5. В информационной системе должны обеспечиваться проверка работоспособности, актуальность базы данных признаков компьютерных вирусов

и версии программного обеспечения средств антивирусной защиты.

6.2.6. В информационной системе должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы.

6.2.7. В информационной системе должна обеспечиваться регистрация событий о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов).

6.2.8. В Учреждении должна обеспечиваться антивирусная защита на этапе инициализации микропрограммного обеспечения средства вычислительной техники.

6.3. Правила и процедуры антивирусной защиты информационной системы регламентируются в настоящей Инструкции и устанавливают:

6.3.1. Безопасность аппаратно- программного обеспечения в Министерстве от разрушающего воздействия компьютерных вирусов достигается также проведением мероприятий по антивирусной защите, основанных на следующих принципах:

6.3.1.1. контроль состояния антивирусной защиты ИС Учреждении возлагается на администратора безопасности информации или уполномоченное лицо;

6.3.1.2. к использованию в ИС допускаются только сертифицированные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств;

6.3.1.3. в информационных системах ежедневно в начале работы при загрузке компьютеров в автоматическом режиме обязан проводиться автоматический контроль всех дисков и файлов;

6.3.1.4. должно обеспечиваться автоматическое централизованное обновление вирусных сигнатур и антивирусного ПО на всех ПЭВМ, работающих в ИС;

6.3.1.5. обязательному автоматическому антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных (несъемных) носителях (магнитных дисках, CD-ROM, флэш и т.п.);

6.3.1.6. разархивирование и контроль входящей информации обязан проводиться непосредственно после ее приема на выделенном автономном компьютере или на любом другом компьютере (возможно применение другого способа антивирусного контроля входящей информации, обеспечивающей аналогичный уровень эффективности контроля);

6.3.1.7. контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный машинный носитель информации);

6.3.1.8. файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль;

6.3.1.9. периодические проверки электронных архивов должны проводиться

не реже одного раза в месяц;

6.3.1.10. устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

VII. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

7.1. Администратором безопасности информации (программистом) должны выполняться следующие требования Регуляторов к реализации обновления базы данных признаков вредоносных компьютерных программ (вирусов):

7.1.1. Администратором безопасности информации (программистом) должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов). Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
- получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

7.2. Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в настоящей Инструкции.

7.3. Администратором безопасности информации (программистом) должны выполняться следующие требования Регуляторов к усилению мероприятий по обновлению базы данных признаков вредоносных компьютерных программ (вирусов):

7.3.1. В информационных системах должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

7.3.2. В информационной системе должно обеспечиваться автоматическое обновление базы данных признаков вредоносных компьютерных программ (вирусов) на всех компонентах информационной системы.

7.3.3. В информационной системе должен обеспечиваться запрет изменений настроек системы обновления базы данных признаков вредоносных компьютерных программ (вирусов) на автоматизированных рабочих местах и серверах.

7.3.4. В информационной системе должна обеспечиваться возможность возврата (отката) к предыдущим обновлениям базы данных признаков вредоносных компьютерных программ (вирусов).

VIII. Действия пользователей при подозрении на вирусную атаку средств вычислительной техники информационной системы

8.1. При возникновении подозрения на наличие компьютерного вируса

(нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках и т.п.) пользователь вместе с администратором безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции.

8.2. В случае обнаружения при проведении антивирусной проверки файлов, зараженных компьютерными вирусами, пользователь обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации, владельца зараженных файлов, а также работников, использующих эти файлы в работе;

- совместно с владельцем зараженных файлов провести анализ необходимости дальнейшего их использования.

8.3. Пользователь совместно с администратором безопасности информации (программистом) проводит лечение или уничтожение зараженных файлов. Администратором безопасности информации (программистом) проводятся мероприятия по закрытию инцидента информационной безопасности.

8.4. По закрытию инцидента информационной безопасности администратором безопасности информации (программистом) проводятся:

8.4.1. по указанию руководителя Учреждения служебная проверка по выяснению причин инцидента информационной безопасности и виновных в нем; анализ причин возникновения инцидента.

IX. Методы обнаружения и устранения компьютерных вирусов

9.1. Сканирование является самым простым программным методом поиска КВ. При данном методе поиска необходимо учитывать, что:

- Антивирусные программы-сканеры могут гарантированно обнаружить только уже известные компьютерные вирусы, которые были предварительно изучены и для которых была определена сигнатура.

- Для эффективного использования антивирусных программ, реализующих метод сканирования, необходимо постоянно обновлять их, получая самые последние версии.

9.2. Метод обнаружения изменений основан на использовании антивирусных программ-ревизоров, которые запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, параметры всех контролируемых файлов, а также информацию о структуре каталогов и номера плохих кластеров диска. Могут быть проверены и другие характеристики компьютера: объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры. При данном методе поиска необходимо учитывать, что:

- Программы-ревизоры потенциально могут обнаружить любые КВ, даже те, которые ранее не были известны. Однако следует учитывать, что не все изменения вызваны вторжением КВ. Так, загрузочная запись может измениться при обновлении версии операционной системы, а некоторые программы записывают

изменяемые данные внутри своего выполнимого файла. Командные файлы изменяются еще чаще; так, например, файл AUTOEXEC.BAT обычно изменяется во время установки нового программного обеспечения.

- Программы-ревизоры не помогут и в том случае, когда пользователь записывает в компьютер новый файл, зараженный КВ. При этом, если КВ заразит другие программы, уже учтенные ревизором, он будет обнаружен.

- Дополнительной возможностью программ-ревизоров является способность восстановить измененные (зараженные) файлы и загрузочные секторы на основании запомненной ранее информации.

- Антивирусные программы-ревизоры нельзя использовать для обнаружения КВ в файлах документов, так как эти файлы постоянно изменяются. Поэтому для контроля за данными файлами следует использовать программы-сканеры или эвристический анализ.

9.3. Эвристический анализ позволяет обнаруживать ранее неизвестные КВ, причем для этого не надо предварительно собирать данные о файловой системе, как требует метод обнаружения изменений. К основным недостаткам эвристического метода относятся следующие:

- принципиально не могут быть обнаружены все КВ;

- возможно появление некоторого количества ложных сигналов об обнаружении КВ в программах, использующих вирусоподобные технологии (например, антивирусы).

9.4. Большинство резидентных сторожей позволяет автоматически проверять все запускаемые программы на заражение известными КВ. Такая проверка будет занимать некоторое время, и процесс загрузки программы замедлится, но зато пользователь будет уверен, что известные КВ не смогут активизироваться на его компьютере. К недостаткам метода резидентных сторожей относятся:

- Многие программы, даже не содержащие КВ, могут выполнять действия, на которые реагируют резидентные сторожа. Например, обычная команда LABEL изменяет данные в загрузочном секторе и вызывает срабатывание сторожа. Поэтому работа пользователя будет постоянно прерываться раздражающими сообщениями антивируса. Кроме того, пользователь должен будет каждый раз решать, вызвано ли это срабатывание компьютерным вирусом или нет. Как показывает практика, рано или поздно пользователь отключает резидентный сторож.

- Следующий недостаток резидентных сторожей заключается в том, что они должны быть постоянно загружены в оперативную память и, следовательно, уменьшают объем памяти, доступной другим программам.

9.5. Основными недостатками метода вакцинирования являются возможность обхода такой защиты при использовании компьютерным вирусом так называемой "стелс-технологии", а также необходимость изменения кода программ, из-за чего некоторые программы начинают работать некорректно или могут перестать работать.

9.6. Аппаратно-программные методы представляют собой один из самых

надежных способов защиты ПС от заражения КВ. Благодаря тому, что контроллер такой защиты подключен к системной шине компьютера, он получает полный контроль над всеми обращениями к дисковой подсистеме компьютера. Программное обеспечение аппаратной защиты позволяет указать области файловой системы, которые нельзя изменять. Пользователь может защитить главную загрузочную запись, загрузочные секторы, выполнимые файлы, файлы конфигурации и т.д. Если аппаратно-программный комплекс обнаружит, что какая-либо программа пытается нарушить установленную защиту, он может не только сообщить об этом пользователю, но и заблокировать дальнейшую работу компьютера. Аппаратный уровень контроля за дисковой подсистемой компьютера не позволяет КВ замаскировать себя. Как только КВ проявит себя, он сразу будет обнаружен. При этом совершенно безразлично, как именно "работает" КВ и какие средства он использует для доступа к дискам и дискетам. Аппаратно-программные средства защиты позволяют не только защитить компьютер от КВ, но также вовремя пресечь выполнение программ, нацеленных на разрушение файловой системы компьютера. Кроме того, аппаратно-программные средства позволяют защитить компьютер от неквалифицированного пользователя, не давая ему удалить важную информацию, переформатировать диск, изменить файлы конфигурации.

9.7. Недостатком аппаратно-программных методов является принципиальная возможность пропустить КВ, если они не пытаются изменять защищенные файлы и системные области.

X. Ответственность и полномочия персонала

10.1. Ответственность персонала

10.1.1. Ответственность за осуществление антивирусного контроля в ИС Учреждения в соответствии с требованиями Инструкции возлагается на администратора безопасности информации (программиста).

10.1.2. За нарушение требований Инструкции администраторы (программисты) и пользователи несут уголовную, административную, гражданско-правовую и дисциплинарную ответственность в соответствии с действующим законодательством.

10.2. Полномочия персонала

10.2.1. Сотрудники Учреждения имеют право выходить с предложениями к руководителю Учреждения по вопросам защиты конфиденциальной информации.

XI. Заключительные положения

11.1. Изменения в настоящую Инструкцию вносятся приказом Учреждения после обязательного согласования вносимых изменений с ответственным за организацию обработки персональных данных в Учреждении, и ответственным за организацию обеспечения безопасности информации в информационных системах Учреждения, отвечающими за соответствие вносимых изменений требованиям

законодательства и нормативно- правовых актов Регуляторов.

11.2. Положения настоящей Инструкции применяются совместно с положениями Порядка обращения с конфиденциальной информацией и средствами криптографической защиты в Учреждении от 1 июня 2016 года № 781.

11.3. Положения настоящей Инструкции имеют приоритет над положениями указанного Порядка.