**Муниципальное бюджетное общеобразовательное учреждение города Владимира «Средняя общеобразовательная школа № 24»**
600028 г. Владимир, улица Лакина, д. 183, тел./факс (84922) 33-61-00,
e-mail: shkvlad24@yandex.ru сайт школы: http://t30862l.sch.obrazovanie33.ru/
Директор школы: Старостина Татьяна Владимировна

| «ПРИНЯТО» | «СОГЛАСОВАНО» | «УТВЕРЖДАЮ» |
|---|---|---|
| на педагогическом совете | председатель Совета родителей школы | директор МБОУ «СОШ №24» г.Владимира |
| МБОУ «СОШ № 24» г.Владимира | 30.08.2023г. пр. № 4 | приказ № 184-од от 31.08.2023г. |
| 30.08.2023г. пр. № 9 | | |
| секр. С.Г. Сильянова | О.В. Журавлева | Т.В. Старостина |

# 2.27. ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ГОРОДА ВЛАДИМИРА «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 24»

Старостина Татьяна Владимировна
Подписано цифровой подписью: Старостина Татьяна Владимировна
Дата: 2023.10.12 17:35:11 +03'00'

## 1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Положение об информационной безопасности МБОУ «СОШ № 24» (далее – Положение) регламентирует единые требования по обеспечению информационной безопасности МБОУ «СОШ № 24» (далее – школа) при использовании ресурсов и каналов передачи данных сети «Интернет» и определяет их полномочия, обязанности и ответственность.

1.2. Настоящее Положение разработано на основе следующих нормативно-правовых документов:

- Федерального закона от 29.12.2012 года № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);
- Федерального закона от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» » (с изменениями и дополнениями);
- Постановления Правительства РФ от 15 июля 2022 г. N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)"
- Распоряжения Правительства РФ от 28 апреля 2023 г. N 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации»;
- Письма Минпросвещения России от 07.06.2019 № 04-474 «О методических рекомендациях»;
- Письма Министерства образования и науки РФ от 28 апреля 2014 г. N ДЛ-115/03 "О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет";
- Устава МБОУ «СОШ № 24».

## 2. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Информационная безопасность направлена на защиту единого информационного образовательного пространства школы от незаконного проникновения, на предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации, а также недопущения доступа обучающихся и работников учреждения к информации, которая запрещена или ограничена к распространению в Российской Федерации.

2.2. Информационная безопасность школы направлена на решение следующих задач:

2.2.1. защита прав и законных интересов обучающихся в образовательной деятельности, защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию и (или) не соответствующей задачам образования;

2.2.2. разграничение объемов и содержания информации, которая может быть доступна различным категориям пользователей;

2.2.3. предотвращение утечки, хищения, утраты, подделки информации школы;

2.2.4. предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации школы;

2.2.5. предотвращение других форм незаконного вмешательства в информационные ресурсы школы.

## 3. ОРГАНИЗАЦИОННО-АДМИНИСТРАТИВНЫЕ МЕРЫ, НАПРАВЛЕННЫЕ НА ЗАЩИТУ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И (ИЛИ) РАЗВИТИЮ

3.1. Приказом директора в школе назначается лицо, ответственное за обеспечение информационной безопасности с полномочиями, определенными соответствующей инструкцией (Приложение 1).

3.2. В школе разрабатываются и утверждаются локальные нормативные акты, регламентирующие:

3.2.1. политику обработки персональных данных, права и обязанности обучающихся и работников школы в сфере защиты персональных данных;

3.2.2. порядок доступа и использования сети Интернет в школе;

3.2.3. организацию контроля использования сети Интернет в школе;

3.2.4. организацию контроля за библиотечным фондом и предотвращение доступа обучающихся к информации экстремистского характера, к информации, запрещенной для распространения среди детей и (или) не соответствующей возрасту обучающихся.

3.3. В школе оказывается организационная и методическая поддержка работникам в области безопасной работы с информационными ресурсами, информационными образовательными технологиями, в том числе, путем их направления на повышение квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети Интернет (Приложение 2).

3.4. В школе на регулярной основе осуществляется информирование работников, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации, локальных актов школы по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет».

3.5. В школе разрабатывается, реализуется и совершенствуется комплекс мероприятий, направленный на правовое просвещение обучающихся и родителей (законных представителей) несовершеннолетних обучающихся в сфере информационной

безопасности, на формирование навыков обучающихся безопасной работы в информационно-телекоммуникационных сетях.
3.6. Жалобы или претензии о нарушениях законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, включая несоответствие применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, установленным законодательством требованиям, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, и направление мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий рассматриваются руководством школы в срок, не превышающий 7 (семи) рабочих дней со дня получения.
3.7. В случае получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, установление причин и условий возникновения такого доступа и принятие мер по их устранению осуществляется руководством школы незамедлительно.

## 4. ИНФОРМАЦИЯ, ИСПОЛЬЗУЕМАЯ В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ И КОНТРОЛЬ ЗА ЕЕ СОДЕРЖАНИЕМ

4.1. Информация и (или) информационная продукция, используемая в образовательной деятельности, осуществляемой в школе, должна соответствовать требованиям законодательства Российской Федерации к защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствовать содержанию и задачам образования.
4.2. При осуществлении образовательной деятельности в школе обеспечивается доступ обучающихся и работников к:

4.2.1. печатной продукции, которая входит в библиотечный фонд школы;

4.2.2. электронным образовательным ресурсам, прошедшим педагогическую экспертизу, рекомендованным и (или) сформированным органами государственной власти, осуществляющими управление в сфере образования.

4.2.3. общедоступным государственным и региональным информационным системам;

4.2.4. информационно-телекоммуникационной сети Интернет в порядке, установленном локальным нормативным актом школы.

4.3. В работе и (или) общении с обучающимися педагогическим работникам или иным работникам школы не допускается использовать информацию:

4.3.1. которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иную информацию, за распространение которой предусмотрена уголовная или административная ответственность;

4.3.2. запрещенную для распространения среди детей;

4.3.3. имеющую знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся);

4.3.4. полученную с нарушением авторских или смежных прав;

4.3.5. имеющую конфиденциальный характер в соответствии с действующим законодательством и (или) локальными нормативными актами школы.

4.4. В образовательной и (или) досуговой деятельности с обучающимися, организуемой и проводимой работниками школы, не допускается посещения зрелищных или иных мероприятий, билеты на которые (афиши или иная информация о мероприятии) содержат знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся).
4.5. В процессе осуществления образовательной деятельности с использованием информационно-компьютерных технологий педагогическими работниками осуществляется контроль за использованием обучающимися сети Интернет, в том числе, визуальный контроль.

4.6. При обнаружении угроз информационной безопасности школы, несанкционированного доступа к локальной сети, а также обнаружении доступа к ресурсу, содержание которого может нанести вред здоровью и (или) развитию обучающихся, работники школы обязаны незамедлительно сообщить об этом руководству для принятия соответствующих мер.

## 5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ФОРМИРОВАНИЮ БЕЗОПАСНЫХ УСЛОВИЙ ДОСТУПА ОБУЧАЮЩИХСЯ К РЕСУРСАМ СЕТИ ИНТЕРНЕТ

5.1. В школе обеспечивается антивирусная защита компьютерной техники, систематически проводится обновление антивирусных программ.
5.2. Для приобретения и использования программного обеспечения в образовательной и иной деятельности школы проводится проверка его подлинности.
5.3. В школе не допускается обучающимися и работниками, а также иными лицами самовольная установка программного обеспечения на компьютерную технику школы, либо использование не принадлежащих школе программ и оборудования.

## 6. ОБУЧЕНИЕ И ПРОСВЕЩЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В рамках образовательной деятельности в школе осуществляется обучение безопасным способам работы в информационно-телекоммуникационных сетях, в план воспитательной работы школы включаются мероприятия, направленные на повышение медиаграмотности обучающихся, формированию навыков безопасного поведения в сети Интернет.
6.2. В школе проводятся образовательные и консультационные мероприятия с родителями (законными представителями) обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет.
6.3. На информационном стенде и в кабинетах, оснащенных персональными устройствами для выхода в сеть Интернет, размещаются информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.
6.4. На официальном сайте школы размещается специализированный раздел «Информационная безопасность», в рамках которого предусмотрено размещение локальных нормативных актов в сфере обеспечения информационной безопасности обучающихся, нормативно-правовых документов, регламентирующих обеспечение информационной безопасности несовершеннолетних, методические рекомендации, информационные памятки для работников, обучающихся и их родителей (законных представителей), направленные на повышение информационной грамотности и обеспечение информационной безопасности детей.

## 7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

7.1. Положение вступает в силу с момента его утверждения приказом директора школы.
7.2. Положение отменяется или изменяется в случае изменения действующего законодательства, а также при наличии иных нормативно-правовых оснований, влекущих изменение, дополнение или отмену закрепленных в нем положений.
7.3. Положение размещается на информационном стенде школы и на официальном сайте школы в сети Интернет.

Приложение 1
к Положению 2.27.

# Инструкция
# администратора безопасности информационных систем персональных данных

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности (далее – АБ) в информационных системах персональных данных (далее – ИСПДн) Муниципального бюджетного образовательного учреждения города Владимира «Средняя общеобразовательная школа № 24» (далее – Учреждение).

1.2. Субъектами доступа к ресурсам ИСПДн являются пользователи, АБ и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт), в соответствии с утвержденным перечнем.

1.3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4. Машинные носители с защищаемой информацией имеют пометку «ПДн».

1.5. АБ назначается Приказом Директора Учреждения и получает неограниченные права на доступ к ресурсам ИСПДн.

1.6. АБ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИСПДн и обслуживающего персонала.

1.7. Методическое руководство по информационной безопасности объектов информатизации осуществляет АБ.

1.8. АБ имеет право вносить предложения по изменению и дополнению данной Инструкции, а также «Инструкции пользователя…» и «Инструкции обслуживающего персонала…».

1.9. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.10. Право толкования положений настоящей Инструкции возлагается на Директора Учреждения.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Доступ к информации – возможность получения информации и ее использования.

2.2. Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.3. Информация – сведения (сообщения, данные) независимо от формы их представления.

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

2.5. Несанкционированный доступ – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.6. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

2.7. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.9. Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.10. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

## 3. ТРЕБОВАНИЯ К АБ

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

3.2. АБ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПДн не допускается.

3.3. АБ осуществляет учет съемных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

3.4. АБ обязан немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее – ОТСС и ВТСС), СЗИ, системного и прикладного программного обеспечения (далее – ПО) ИСПДн.

3.5. АБ обязан немедленно ставить в известность ответственного за обеспечение безопасности персональных данных Учреждения обо всех неисправностях аппаратно-программных средств ИСПДн.

3.6. АБ обязан ставить в известность ответственного за обеспечение безопасности персональных данных Учреждения о необходимости проведения работ по администрированию СЗИ.

3.7. АБ имеет право проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

3.8. АБ разрабатывает планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ИСПДн Учреждения.

3.9. АБ обязан в случае отказа технических средств или программного обеспечения элементов ИСПДн, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.10. АБ имеет право требовать прекращения обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

3.11. АБ присутствует при выполнении технического обслуживания элементов ИСПДн сторонними специалистами на территории Учреждения.

3.12. АБ осуществляет разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе с СЗИ, или по

другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.13. В ходе управления (администрирования) системой защиты ИСПДн АБ обязан осуществлять:

3.13.1. заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИСПДн и поддержание правил разграничения доступа в ИСПДн;

3.13.2. создание, присвоение и уничтожение идентификаторов пользователей и устройств, однозначно их идентифицирующих;

3.13.3. управление СЗИ в ИСПДн, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

3.13.4. изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИСПДн;

3.13.5. установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

3.13.6. централизованное управление системой защиты информации ИСПДн (при необходимости);

3.13.7. регистрацию и анализ событий в ИСПДн, связанных с защитой информации;

3.13.8. информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПДн и отдельных СЗИ, а также их обучение;

3.13.9. сопровождение функционирования системы защиты информации ИСПДн в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

3.14. В ходе выявления инцидентов и реагирования на них АБ обязан осуществлять:

3.14.1. обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.14.2. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДн;

3.14.3. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

3.14.4. планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.14.5. планирование и принятие мер по предотвращению повторного возникновения инцидентов.

3.15. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн, АБ обязан осуществлять:

3.15.1. анализ и оценку функционирования системы защиты информации ИСПДн, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИСПДн;

3.15.2. проверку работоспособности и параметров настройки программного обеспечения, аппаратных и программных СЗИ ИСПДн;

3.15.3. проверку состава технических средств, программного обеспечения и СЗИ;

3.15.4. контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных;

3.15.5. еженедельное отслеживание появления новых видов уязвимостей ПО ИСПДн. По необходимости АБ производит устранение уязвимостей согласно рекомендациям разработчика, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств. В качестве источников информации об уязвимостях должны использоваться опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей;

3.15.6. периодический анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

3.15.7. контроль за событиями безопасности и действиями пользователей в ИСПДн. В частности, АБ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;

3.15.8. контроль (анализ) защищенности информации, содержащейся в ИСПДн;

3.15.9. документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн;

3.15.10. принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИСПДн, повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

## 4. ДОСТУП К РЕСУРСАМ ИСПДН

4.1. Обязательными условиями получения доступа к ресурсам ИСПДн АБ являются:

- право доступа в помещение;
- наличие допуска к персональным данным;
- право доступа к ИСПДн;
- знание технологии обработки информации в ИСПДн с учетом требований информационной безопасности.

4.2. Идентификация АБ в ИСПДн осуществляется по уникальному имени и персональному идентификатору (при его наличии).

4.3. Длина пароля АБ и всех пользователей – не менее 6 буквенно-цифровых символов.

4.4. Уникальное имя, персональный идентификатор (при его наличии) и пароль АБ получает в установленном порядке. АБ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

4.5. При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

4.6. Регистрация пользователя осуществляется АБ в соответствии с «Инструкцией по организации парольной защиты» и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

4.7. При заведении новой учетной записи, АБ должен проверить личность пользователя и его трудовые обязанности.

4.8. Пересмотр и, при необходимости, корректировка учетных записей пользователей производится АБ не реже одного раза в 6 месяцев и по мере необходимости.

4.9. Предоставление пользователям прав доступа к объектам доступа ИСПДн должно осуществляться на основании задач, решаемых пользователями.

4.10. АБ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

4.11. АБ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

## 5. ПОРЯДОК РАБОТЫ АБ С РЕСУРСАМИ ИСПДН

Ниже приводится перечень работ, производимых АБ с ресурсами ИСПДн.

5.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн АБ присваивает пользователям идентификационные данные к ресурсам ИСПДн. При этом должны выполняться следующие требования:

- АБ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;
- АБ сообщает пользователю его уникальное имя и предоставляет возможность

задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;

- изменение учетных данных пользователя производится АБ по требованию ответственного за обеспечение безопасности персональных данных Учреждения, а также периодически по утвержденному плану и в случае увольнения работника;
- АБ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АБ обязан потребовать у пользователя изменение пароля.

5.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ) АБ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить. В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБ обязан приостановить обработку защищаемой информации до устранения неисправности. В случае производственной необходимости – отключить СЗИ и лично контролировать проведение работ пользователями.

5.3. Антивирусная защита ресурсов ИСПДн АБ разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры антивирусной программы;
- контролирует работоспособность антивирусной программы;
- немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;

- имеет право на проведение внеплановой проверки на наличие вирусов;
- периодически (один раз в неделю) контролирует корректность процесса обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

5.4. Хранение дистрибутивов программного обеспечения СЗИ. АБ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИСПДн Учреждения в месте, исключающем доступ посторонних лиц.

5.5. Проверка целостности системного и прикладного ПО. Контролю целостности подлежат файлы ПО ИСПДн с расширениями: *.exe, *.com, *.dll, *.sys, *.vxd, *.drv из каталогов: Windows, Program Files.

5.6. Резервное копирование и восстановление информации Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

- обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых машинных носителей (далее – МН);
- допускается обоснованное внеплановое резервное копирование информации как по инициативе пользователя, так и АБ, если это не нарушает технологию обработки информации;
- резервные копии пользовательской информации и информации операционной системы хранятся на учтенных внешних МН;
- ответственным лицом за хранение резервных копий является АБ.

По мере устранения неисправностей ПЭВМ АБ производит восстановление информации ограниченного доступа с резервных копий. Восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), производится, в том числе с использованием резервных копий и (или) дистрибутивов.

АБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5.7. Конфигурирование ИСПДн Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр. Управление изменениями конфигурации осуществляет ответственный за обеспечение безопасности. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБ. В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации АБ обязан осуществлять:

- поддержание конфигурации ИСПДн и ее системы защиты информации (структуры системы защиты информации ИСПДн, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПДн и ее системы защиты информации);
- управление изменениями базовой конфигурации ИСПДн и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПДн и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПДн и ее системы защиты информации,

контроль действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

- анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДн и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

- определение параметров настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

- внесение информации (данных) об изменениях в базовой конфигурации ИСПДн и ее системы защиты информации в документацию на систему защиты информации ИСПДн;

- принятие решения по результатам управления конфигурацией о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБ. При возникновении необходимости изменения конфигурации ИСПДн, аттестованной по требованиям безопасности информации, АБ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

5.8. Вывод ресурсов ИСПДн из эксплуатации. При невозможности ремонта различных ресурсов ИСПДн АБ обязан:

- физически уничтожать любые МН, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИСПДн;

- факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ИСПДн.

5.9. Реагирование на сбои при регистрации событий безопасности. Реагирование на сбои при регистрации событий безопасности осуществляется АБ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности, АБ обязан:

- немедленно уведомить Директора о данном факте;
- по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;
- восстановить работоспособность ИСПДн;
- по окончании работ по восстановлению работоспособности ИСПДн произвести запись в соответствующих журналах.

## 6. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

6.1. К попыткам несанкционированного доступа относятся:

- сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

- действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или

другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

6.2. При выявлении факта несанкционированного доступа АБ обязан:

- пресечь дальнейший несанкционированный доступ к ИСПДн;
- доложить ответственному за обеспечение безопасности персональных данных Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
- известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

## 7. ОТВЕТСТВЕННОСТЬ

7.1. АБ несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации в рабочее время;
- несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИСПДн;
- средства защиты информации, применяемые в ИСПДн Учреждения;
- качество проводимых работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени учетной записи АБ в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

7.2. АБ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 2
к Положению 2.27.

# Инструкция Пользователя СКЗИ МБОУ «СОШ № 24»

## 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. В настоящей Инструкции применяются следующие термины и определения:

- **Доступ к информации** - возможность получения информации и ее использования.
- **Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
- **Информация ограниченного доступа** - информация, доступ к которой ограничен федеральными законами.
- **Исходная ключевая информация** - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.
- **Ключевая информация** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.
- **Ключевой блокнот** - набор бумажных ключевых документов одного вида (таблиц, перфолент, перфокарт и т.п.), сброшюрованных и упакованных по установленным правилам.
- **Ключевой документ** - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.
- **Ключевой носитель** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт - диск, Data Key, Smart Card, Touch Memory и т.п.).

- **Компрометация криптоключей** – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.
- **Контролируемая зона** - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.
- **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
- **Криптографический ключ (криптоключ)** - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.
- **Лицензиат ФСБ** – оператор конфиденциальной связи и лица, имеющие лицензию ФСБ и не являющиеся операторами конфиденциальной связи.
- **Орган криптографической защиты** – организация, структурное подразделение организации - лицензиата ФСБ России.
- **Пользователи СКЗИ** – физические лица, непосредственно допущенные к работе с СКЗИ.
- **Средства криптографической защиты информации (СКЗИ)** – сертифицированные ФСБ (ФАПСИ) России средства:
  - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно - программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;
  - реализующие криптографические алгоритмы преобразования информации

аппаратные, программные и аппаратно - программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно - программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и «электронной подписи»;

- аппаратные, программные и аппаратно - программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.

- **Специализированные помещения** - помещения, где установлены СКЗИ или хранятся ключевые документы к ним.

## 2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая инструкция определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, в целях обеспечения безопасности эксплуатации СКЗИ в МБОУ «СОШ № 24» (далее – Учреждение).

2.2. Настоящая Инструкция разработана в соответствии с:

- Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66;

- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну от 13 июня 2001 г. №152;

- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными ФСБ России от 21 февраля 2008 г. № 149.

2.3. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами назначается Администратор безопасности, имеющий необходимый уровень квалификации, назначаемый приказом руководителя Учреждения (далее – АБ). АБ осуществляет:

- поэкземплярный учет СКЗИ;

- контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;

- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации.

2.4. Пользователи СКЗИ назначаются приказом руководства Учреждения.

2.5. Пользователь СКЗИ обязан:

- строго соблюдать правила пользования СКЗИ и требования настоящей Инструкции;

- не допускать установки на ПЭВМ нештатных программ, предупреждать возможность занесения вирусов и других вредоносных программ;

- не разглашать информацию, к которой они допущены, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;

- соблюдать требования к обеспечению безопасности информации ограниченного доступа, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- немедленно уведомлять АБ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы - в соответствии с установленным порядком, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- не допускать снятие копий с ключевых документов;

- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер; - не допускать записи на ключевой носитель посторонней информации;

- не допускать установки ключевых документов в другие ПЭВМ.

2.6. Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения. Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты.

2.7. Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на АБ.

2.8. АБ и Пользователи СКЗИ должны быть ознакомлены с Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными ФСБ России от 21 февраля 2008 г. № 149 и настоящей Инструкцией под расписку.

## 3. УЧЕТ, ХРАНЕНИЕ СКЗИ И КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

3.1. Учет криптографических средств.

3.1.1. Криптосредства, эксплуатационная и техническая документация к ним, используемые для обеспечения безопасности информации ограниченного доступа, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

3.1.2. Все поступившие СКЗИ, эксплуатационная и техническая документации к ним должны быть взяты на поэкземплярный учет по Журналу поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

3.1.3. Поэкземплярный учет СКЗИ имеет цель обеспечить контроль за снабжением СКЗИ, их наличием, движением, расходованием и исключить обезличенное пользование ими. В журнале поэкземплярного учета должно отражаться полное прохождение каждого в отдельности экземпляра СКЗИ, эксплуатационной и технической документации к ним с момента получения до уничтожения.

3.1.4. Единицей поэкземплярного учета криптографических средств, ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.1.5. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет АБ.

3.1.6. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются под расписку в соответствующем журнале поэкземплярного учета Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

3.1.7. При увольнении, перемещении Пользователя СКЗИ все числящие за ним СКЗИ и другие документы передаются по акту сотруднику, которому поручено исполнять его обязанности. При временном убытии сотрудника (в том числе командировку, отпуск, по болезни) по акту могут быть переданы только СКЗИ и документы, необходимые для работы в период его отсутствия. Остальные числящие СКЗИ и документы должны находиться в хранилище (упаковке), опечатанном его личной печатью. Акты составляются в одном экземпляре.

3.2. Хранение криптографических средств.

3.2.1.Незадействованные в эксплуатации СКЗИ, дистрибутивы СКЗИ на магнитных носителях, эксплуатационная и техническая документация к ним хранится у АБ. Криптографические ключи хранятся у Пользователей СКЗИ.

3.2.2.Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-програмные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.2.3.Инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к СКЗИ, ключевые документы хранятся в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.2.4.Действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, хранятся раздельно.

3.3. Рассылка СКЗИ, ключевых документов.

3.3.1.Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными ответственными Пользователями СКЗИ и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки. Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

3.3.2.Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

3.3.3.Полученные упаковки вскрывают пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю.

3.3.4.При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний изготовителя.

3.3.5.Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме.

3.4. Уничтожение СКЗИ, ключевых документов.

3.4.1.СКЗИ уничтожают (утилизируют) в соответствии с требованиями эксплуатационной и технической документации к ним.

3.4.2.Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и

технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

3.4.3.Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

3.4.4.СКЗИ, ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета.

3.4.5.О проведенном уничтожении СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, делаются отметки в соответствующих журналах учета.

3.4.6.Не реже одного раза в год пользователи СКЗИ должны направлять в орган криптографической защиты письменные отчеты об уничтоженных ключевых документах.

3.5. Компрометация криптоключей.

3.5.1.Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают в соответствующий орган криптографической защиты. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению органа криптографической защиты, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

3.5.2.О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации, пользователи СКЗИ обязаны сообщать в соответствующий орган криптографической защиты. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.5.3.Необходимо провести мероприятия по розыску и локализации последствий компрометации информации, передававшейся (хранящейся) с использованием СКЗИ.

3.5.4. Размещение, охрана и организация режима в помещениях, где установлены СКЗИ

3.6. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее – специализированные помещения), должны обеспечивать сохранность информации ограниченного доступа, криптосредств и ключевых документов к ним.

3.7. При оборудовании специализированных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с криптосредствами.

3.8. Специализированные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное

закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

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

3.10. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает АБ по согласованию с руководством Учреждения. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны. Внутриобъектовый режим устанавливается отдельной инструкцией.

3.11. Для предотвращения просмотра извне специализированных помещений их окна должны быть защищены.

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

3.13. На время отсутствия Пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с АБ необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

3.14. В специализированных помещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

3.15. При утрате ключа от хранилища или от входной двери в специализированное помещение пользователя СКЗИ замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

3.16. В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

3.17. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в специализированное помещение или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству Учреждения и руководителю органа криптографической защиты. Прибывшие сотрудники органа криптографической защиты должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей