

ГОСУДАРСТВЕННОЕ КАЗЁННОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ
«СПЕЦИАЛЬНАЯ БИБЛИОТЕКА КУЗБАССА
ДЛЯ НЕЗРЯЧИХ И СЛАБОВИДЯЩИХ»

ПРИКАЗ

05.10.2026

№ 53

О назначении ответственных лиц по вопросам защиты информации

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также Приказа ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», в целях обеспечения защиты информации, в том числе персональных данных, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию защиты информации, за обеспечение безопасности персональных данных, за эксплуатацию средств криптографической защиты информации (далее – СКЗИ), за защиту информации в информационных системах (администратор безопасности), за техническое обслуживание информационных систем (администратор системы) – инженера-программиста ГКУК «КузОСБ» Жаурова В. В.
2. Утвердить прилагаемое Положение об ответственном за организацию защиты информации (Приложение № 1).
3. Утвердить прилагаемое Положение об ответственном за защиту информации в информационных системах (Приложение № 2).
4. Утвердить прилагаемое Положение об ответственном за обеспечение безопасности персональных данных (Приложение № 3).
5. Утвердить прилагаемое Положение об ответственном за эксплуатацию средств криптографической защиты информации (Приложение № 4).
6. Утвердить прилагаемое Положение об ответственном за техническое обслуживание информационных систем (Приложение № 5).

7. Утвердить прилагаемое Положение о пользователях информационных систем (Приложение № 6).

8. Назначенному ответственному лицу, а также пользователям информационных систем, в своей работе руководствоваться положениями законодательства Российской Федерации по защите информации, в том числе нормативными и методическими документами ФСТЭК и ФСБ России, а также утверждёнными локальными актами по защите информации.

9. Назначить ответственным за ознакомление с настоящим приказом и положениями заместителя директора ГКУК «КузОСБ» Ветошкину Т. В. Обеспечить доведение документов до всех заинтересованных лиц под роспись.

10. Ответственность и контроль за исполнение настоящего приказа оставляю за собой.

Директор



И. Ю. Тихонова

С приказом ознакомлены:

Науров В.В.
Ветошкина Т.В.

**Положение об ответственном за организацию защиты информации
в государственном казённом учреждении культуры
«Специальная библиотека Кузбасса для незрячих и слабовидящих»**

1. Общие положения

1. Настоящее Положение определяет полномочия, права и обязанности ответственного за организацию защиты информации, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее – ответственное лицо) в государственном казённом учреждении культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее – Организация).

2. Ответственное лицо определяется руководителем Организации.

3. Ответственное лицо осуществляет свою деятельность на основе настоящего Положения и подчиняется непосредственно руководителю Организации либо лицу, его замещающему.

4. Указания и поручения Ответственного лица в части обеспечения защиты информации являются обязательными для исполнения всеми работниками Организации в пределах их компетенции.

5. В своей деятельности ответственное лицо руководствуется: Федеральным законом от 27 июля 2006 г. № 149-ФЗ, Федеральным законом от 27 июля 2006 г. № 152-ФЗ, Федеральным законом от 26 июля 2017 г. № 187-ФЗ, Приказом ФСТЭК России от 11 апреля 2025 г. № 117, иными нормативными и методическими документами ФСТЭК России, ФСБ России, национальными стандартами РФ, Политикой защиты информации, стандартом защиты информации, эксплуатационной документацией на средства защиты информации, настоящим Положением.

2. Квалификационные требования к ответственному лицу

6. Ответственное лицо должно иметь высшее образование (желательно в области информационных технологий или информационной безопасности), либо ответственному лицу рекомендуется пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность» (если организация является субъектом КИИ, то ответственное лицо в обязательном порядке проходит обучение).

7. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:

а) основные (в том числе производственные, бизнес и управленческие) процессы Организации и специфика обеспечения информационной безопасности;

б) влияние информационных технологий на деятельность Организации, в том числе: роль и место информационных технологий в процессах функционирования Организации; зависимость основных процессов от информационных технологий;

в) информационно-телекоммуникационные технологии, в том числе: современные ИТ, способы построения ИС, типовые архитектуры, принципы функционирования ОС, СУБД, сетей, основных протоколов;

г) обеспечение информационной безопасности, в том числе: цели, задачи, основы организации, способы и средства обеспечения ИБ; принципы стратегического развития ИБ; правила разработки документов; порядок организации работ; основные угрозы безопасности информации; возможности типовых средств защиты; порядок взаимодействия структурных подразделений; управление проектами; антикризисное управление; планирование деятельности; разработка и внедрение политики; организация контроля; поддержка и совершенствование деятельности; определение угроз; внедрение средств защиты; анализ и контроль состояния ИБ; обеспечение ИБ на всех этапах жизненного цикла; организация обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3. Трудовые обязанности ответственного лица

8. Ответственное лицо принимает участие в формировании политики Организации, отвечает за согласование стратегии развития организации в части вопросов обеспечения информационной безопасности.

9. Ответственное лицо:

а) организует разработку политики, отвечает за согласование и утверждение политики, реализацию мероприятий, отслеживает и контролирует результаты;

б) организует работу по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

в) организует реализацию и контроль проведения организационных и технических мер, решения о необходимости осуществления которых принимаются ФСБ России и ФСТЭК России;

г) организует беспрепятственный доступ (в том числе удалённый) должностным лицам ФСБ России к информационным ресурсам, доступ к которым обеспечивается посредством сети «Интернет», в целях осуществления мониторинга их защищенности;

д) организует взаимодействие с должностными лицами ФСБ России и ее территориальных органов, контроль исполнения указаний, данных по результатам мониторинга;

е) организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации;

ё) организует развитие информационной безопасности, формирование и развитие навыков работников Организации в сфере информационной безопасности;

ж) организует разработку и реализацию мероприятий по обеспечению информационной безопасности в Организации в соответствии с требованиями к обеспечению информационной безопасности, установленными федеральными законами и иными нормативными правовыми актами;

з) организует контроль пользователей информационных ресурсов в части соблюдения ими режима конфиденциальности, правил работы со съемными носителями, выполнения организационных и технических мер;

и) организует планирование мероприятий по обеспечению информационной безопасности в Организации, подведомственных организациях;

к) организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

л) организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности;

м) организует проведение контроля за состоянием обеспечения информационной безопасности в Организации, подведомственных организациях, включая оценку защищенности систем и сетей.

10. Ответственное лицо:

а) осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в Организации, отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня ИБ;

б) осуществляет регулярное и своевременное информирование руководства Организации о компьютерных инцидентах, текущем уровне ИБ и результатах практических учений по противодействию компьютерным атакам;

в) осуществляет контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым разделам работы;

г) осуществляет согласование требований к системам и сетям в части обеспечения информационной безопасности;

д) осуществляет руководство ответственными лицами (структурным подразделением) Организации, обеспечивающим информационную безопасность.

11. Ответственное лицо:

а) организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности и контролирует их результаты;

б) организует и контролирует функционирование системы обеспечения информационной безопасности, координирует функционирование систем в подведомственных организациях;

в) координирует деятельность иных структурных подразделений, подведомственных организаций по вопросам обеспечения информационной безопасности.

12. Ответственное лицо согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации Организации.

13. В случаях, установленных законодательством, ответственное лицо с использованием нормативных документов и методических материалов ФСБ России организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты, а также взаимодействие с Национальным координационным центром по компьютерным инцидентам одним из способов: силами структурного подразделения (или ответственными лицами) с заключением соглашения о взаимодействии с ФСБ России; силами структурного подразделения с его аккредитацией как центра ГосСОПКА; силами организаций, являющихся аккредитованными центрами ГосСОПКА.

14. В случаях, установленных законодательством, ответственное лицо обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства.

15. Ответственное лицо сопровождает мероприятия по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

16. Ответственное лицо проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в Организации, подведомственных организациях.

17. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности.

18. Ответственное лицо повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

19. Ответственное лицо выполняет иные обязанности, исходя из возложенных полномочий и поставленных руководством задач.

20. Ответственное лицо:

а) соблюдает и обеспечивает выполнение законодательства Российской Федерации;

б) в случаях, установленных законодательством, согласовывает политику с ФСБ России и ФСТЭК России;

в) представляет по запросам ФСБ России и ФСТЭК России достоверные сведения о результатах реализации политики и текущем уровне ИБ;

г) поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности;

д) организывает при необходимости проведение и участвует в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе рабочих групп;

е) участвует в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

4. Права ответственного лица

21. Ответственное лицо имеет право:

а) давать указания и поручения работникам Организации в части обеспечения информационной безопасности;

б) запрашивать от работников информацию и материалы, необходимые для реализации возложенных прав и обязанностей;

в) участвовать в заседаниях (совещаниях) коллегиальных органов Организации, принятии решений по вопросам деятельности, а также по внесению предложений по совершенствованию деятельности;

г) участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу;

д) представлять результаты реализации политики коллегиальному органу;

е) принимать решения по вопросам обеспечения информационной безопасности, в том числе о приостановке эксплуатации ИС (в случае выявления критических угроз);

ё) взаимодействовать с ФСБ России, ФСТЭК России и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности;

ж) вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, к проведению работ по обеспечению информационной безопасности;

з) инициировать проверки уровня обеспечения информационной безопасности в Организации, ее подведомственных и дочерних организациях;

и) организовывать на объектах Организации мероприятия по информационной безопасности, разработку и представление руководителю предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;

к) получать доступ в установленном порядке к сведениям, составляющим государственную тайну, если исполнение обязанностей связано с использованием таких сведений;

л) получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы, органы местного самоуправления, общественные объединения и другие организации;

м) обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей.

5. Ответственность

22. Ответственное лицо в соответствии с законодательством Российской Федерации несёт ответственность:

а) за неисполнение или ненадлежащее исполнение своих обязанностей;

б) за действия (бездействие), ведущие к нарушению прав и законных интересов Организации;

в) за разглашение сведений ограниченного доступа, ставших ему известными в связи с исполнением своих обязанностей;

г) за достижение целей обеспечения информационной безопасности;

д) за поддержание и непрерывное развитие информационной безопасности Организации для исключения негативных последствий;

е) за организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности;

ё) за нарушения требований по обеспечению информационной безопасности;

ж) за нарушения в обеспечении защиты систем и сетей, повлёкшие негативные последствия.

23. Нарушение ответственным лицом требований информационной безопасности влечёт дисциплинарную, административную или уголовную ответственность в порядке, установленном законодательством Российской Федерации.

**Положение об ответственном
за защиту информации в информационных системах
государственного казённого учреждения культуры
«Специальная библиотека Кузбасса для незрячих и слабовидящих»**

1. Общие положения

1. Настоящее Положение определяет статус, задачи, функции, права и ответственность лица, назначаемого ответственным за защиту информации в информационных системах (далее – администратор безопасности), в государственном казённом учреждении культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее – Организация).

2. Администратор безопасности назначается руководителем Организации.

3. Администратор безопасности осуществляет свою деятельность на основе настоящего Положения и подчиняется непосредственно руководителю Организации либо лицу, его замещающему.

4. Указания и поручения администратора безопасности в пределах его компетенции являются обязательными для исполнения пользователями ИС.

5. В своей деятельности администратор безопасности руководствуется: Федеральным законом №149-ФЗ, №152-ФЗ, №187-ФЗ, Приказом ФСТЭК №117, иными нормативными и методическими документами ФСТЭК России, ФСБ России, национальными стандартами РФ, Политикой защиты информации, стандартом защиты информации, эксплуатационной документацией на средства защиты, настоящим Положением.

2. Квалификационные требования

6. Администратор безопасности должен иметь высшее или среднее профессиональное образование. При наличии образования по направлению, не относящемуся к ИТ или ИБ, рекомендуется пройти обучение по программе профессиональной переподготовки в области защиты информации.

7. Администратор безопасности должен обладать знаниями: нормативных правовых актов в области защиты информации; требований Приказа ФСТЭК №117 и методических документов; основных видов угроз безопасности информации; принципов построения ОС, СУБД, сетевых протоколов; порядка установки, настройки и эксплуатации типовых средств защиты информации; методов анализа уязвимостей, управления обновлениями и конфигурациями; порядка регистрации, анализа и реагирования на инциденты.

8. Администратор безопасности должен обладать умениями: управления учётными записями и разграничения доступа; настройки средств защиты; проведения анализа уязвимостей; организации устранения уязвимостей; сбора, регистрации и анализа событий безопасности; взаимодействия с иными должностными лицами; ведения учётных форм и подготовки отчётов.

3. Трудовые обязанности ответственного лица

9. Администратор безопасности выполняет следующие функции:

а) обеспечивает реализацию организационных и технических мер защиты информации в ИС;

б) осуществляет создание, изменение и блокирование учётных записей пользователей и администраторов, ведёт учёт предоставленных прав доступа;

в) контролирует соблюдение правил аутентификации, парольной политики и разделения привилегированных учётных записей;

г) производит установку, настройку и эксплуатацию средств защиты информации (антивирусного ПО, межсетевых экранов, средств контроля доступа, средств защиты от НСД, а во взаимодействии с ответственным за СКЗИ – криптографических средств);

д) обеспечивает соответствие настроек средств защиты утверждённым эталонным конфигурациям, вносит изменения в конфигурацию в установленном порядке;

е) проводит выявление и анализ уязвимостей ИС, оценивает их критичность и принимает меры по устранению выявленных уязвимостей в установленные сроки;

ё) обеспечивает своевременную установку обновлений программного обеспечения, включая средства защиты, и ведёт учёт выполненных обновлений;

ж) осуществляет сбор, регистрацию и анализ событий безопасности, выявляет инциденты информационной безопасности, принимает меры по их локализации;

з) незамедлительно информирует ответственного за организацию защиты информации о выявленных инцидентах и нарушениях;

и) ведёт учётные формы (журналы) в соответствии с требованиями стандарта защиты информации;

к) обеспечивает функционирование антивирусной защиты, контроль актуальности антивирусных баз и проведение сканирований;

л) контролирует соблюдение пользователями установленных правил работы в ИС, пресекает установку несанкционированного ПО;

м) взаимодействует с ответственными за техническое обслуживание ИС по вопросам конфигураций, резервного копирования и восстановления данных, предоставляет требования к безопасной настройке оборудования и ПО;

- н) в случаях, установленных законодательством, обеспечивает техническое взаимодействие с ГосСОПКА в установленном порядке;
- о) подготавливает отчёты о результатах своей деятельности для ответственного за организацию защиты информации, участвует в проведении периодического контроля уровня защищённости;
- п) разрабатывает и актуализирует локальные акты по защите информации.

4. Права ответственного лица

10. Администратор безопасности вправе:

- а) запрашивать и получать от структурных подразделений и должностных лиц информацию, необходимую для выполнения функций;
- б) проводить настройку средств защиты информации в пределах своей компетенции;
- в) блокировать доступ пользователей к ИС при нарушении требований безопасности или при выявлении признаков инцидента с незамедлительным уведомлением ответственного за организацию защиты информации;
- г) требовать от пользователей соблюдения установленных правил работы в ИС;
- д) инициировать проведение внеочередных проверок защищённости, анализа уязвимостей;
- е) вносить предложения руководителю о совершенствовании системы защиты, замене или обновлении средств защиты, проведении дополнительного обучения пользователей;
- ё) привлекать (по согласованию с ответственным за организацию защиты информации) лицензиатов ФСТЭК России для выполнения отдельных работ.

5. Ответственность

11. Администратор безопасности в соответствии с законодательством Российской Федерации несёт ответственность:

- а) за неисполнение или ненадлежащее исполнение возложенных обязанностей;
- б) за несвоевременное или неполное выявление уязвимостей ИС, а также непринятие мер по их устранению в установленные сроки;
- в) за нарушения в настройке средств защиты, повлёкшие снижение уровня защищённости;
- г) за несоблюдение правил управления учётными записями, парольной политики и порядка предоставления доступа;
- д) за несвоевременное или некачественное проведение мониторинга событий безопасности, а также непринятие мер по локализации инцидентов;

е) за несвоевременное информирование ответственного за организацию защиты информации о выявленных инцидентах, нарушениях, изменениях конфигураций;

ё) за разглашение сведений ограниченного доступа, ставших ему известными при исполнении обязанностей;

ж) за нарушение порядка взаимодействия с ГосСОПКА, установленного нормативными правовыми актами и локальными документами.

14. Нарушение администратором безопасности требований информационной безопасности влечёт дисциплинарную, административную или уголовную ответственность.

**Положение об ответственном
за обеспечение безопасности персональных данных
в государственном казённом учреждении культуры
«Специальная библиотека Кузбасса для незрячих и слабовидящих»**

1. Общие положения

1. Настоящее Положение определяет статус, задачи, функции, права и ответственность лица, назначаемого ответственным за обеспечение безопасности персональных данных (далее – ответственный за ПДн), в государственном казённом учреждении культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее – Организация).

2. Ответственный за ПДн назначается руководителем Организации.

3. Ответственный за ПДн осуществляет свою деятельность на основе настоящего Положения и подчиняется непосредственно подчиняется непосредственно руководителю Организации либо лицу, его замещающему.

4. Указания и поручения ответственного за ПДн в пределах его компетенции являются обязательными для исполнения всеми работниками, осуществляющими обработку персональных данных.

5. В своей деятельности руководствуется: ФЗ-149, ФЗ-152, ФЗ-187, Приказом ФСТЭК №117, актами Роскомнадзора, национальными стандартами РФ, Политикой защиты информации, стандартом защиты информации, настоящим Положением.

2. Квалификационные требования

6. Ответственный за ПДн должен иметь высшее или среднее профессиональное образование. При наличии образования по направлению, не относящемуся к ИТ, ИБ или юриспруденции, рекомендуется пройти обучение по программе профессиональной переподготовки в области защиты персональных данных.

7. Ответственный за ПДн должен обладать знаниями: нормативных правовых актов в области персональных данных; порядка ведения учета операций с ПДн, получения и фиксации согласий; принципов разграничения доступа к ПДн; требований к защите ПДн в ИС; порядка взаимодействия с субъектами ПДн; правил ведения документации.

8. Ответственный за ПДн должен обладать умениями: разработки и актуализации локальных актов; ведения реестров согласий и учетных форм; организации контроля за законностью обработки; взаимодействия с

уполномоченными органами; подготовки ответов на обращения субъектов; организации обучения и инструктажа.

3. Трудовые обязанности ответственного лица

9. Ответственный за ПДн выполняет следующие функции:

- а) организует работу по обеспечению защиты персональных данных;
- б) разрабатывает и актуализирует локальные нормативные акты по вопросам обработки и защиты ПДн;
- в) осуществляет контроль за соблюдением установленных требований при обработке ПДн, включая законность оснований, наличие и корректность оформления согласий;
- г) ведёт учёт операций с ПДн (реестры согласий, журналы учета фактов предоставления, журналы уничтожения);
- д) обеспечивает организацию доступа к ПДн в соответствии с установленными правилами, контролирует соблюдение режима конфиденциальности;
- е) организует взаимодействие с субъектами ПДн: принимает и рассматривает запросы, подготавливает ответы;
- ё) организует взаимодействие с уполномоченными государственными органами (Роскомнадзор, ФСТЭК России);
- ж) контролирует проведение мероприятий по технической защите ПДн во взаимодействии с администратором безопасности и системным администратором;
- з) организует проведение обучения и инструктажа работников, участвующих в обработке ПДн;
- и) участвует в расследовании инцидентов, связанных с нарушением обработки или защиты ПДн, принимает меры по минимизации последствий;
- к) обеспечивает документирование фактов нарушения, информирует ответственного за организацию защиты информации и руководителя;
- л) осуществляет контроль за своевременным уничтожением ПДн при достижении целей обработки или отзыве согласия;
- м) подготавливает отчёты о состоянии защиты ПДн для ответственного за организацию защиты информации и руководителя.

4. Права ответственного лица

10. Ответственный за ПДн вправе:

- а) запрашивать и получать от структурных подразделений информацию, необходимую для выполнения функций;
- б) проводить проверки соблюдения установленного порядка обработки ПДн в подразделениях;
- в) давать обязательные для исполнения указания по вопросам обработки и защиты ПДн;

г) требовать от работников соблюдения установленных правил обработки ПДн;

д) инициировать проведение внеплановых проверок, дополнительных мероприятий по защите ПДн при выявлении нарушений;

е) вносить предложения руководителю о совершенствовании системы защиты ПДн, привлечении к дисциплинарной ответственности;

ё) привлекать (по согласованию с ответственным за организацию защиты информации) лицензиатов ФСТЭК России для выполнения работ по оценке защищённости ПДн.

5. Ответственность

11. Ответственный за ПДн в соответствии с законодательством Российской Федерации несёт ответственность:

а) за неисполнение или ненадлежащее исполнение своих обязанностей;

б) за действия (бездействие), ведущие к нарушению прав и законных интересов Организации;

в) за разглашение сведений ограниченного доступа;

г) за несвоевременное или неполное ведение учёта операций с ПДн;

д) за нарушение установленного порядка обработки ПДн, включая неправомерное предоставление доступа;

е) за несвоевременное рассмотрение обращений субъектов ПДн;

ё) за непредоставление или несвоевременное предоставление информации в уполномоченные органы;

ж) за непринятие мер по устранению выявленных нарушений в установленные сроки;

з) за несвоевременное информирование ответственного за организацию защиты информации и руководителя о нарушениях и инцидентах.

12. Нарушение ответственным за ПДн требований влечёт дисциплинарную, административную или уголовную ответственность.

**Положение об ответственном за эксплуатацию средств
криптографической защиты информации
в государственном казённом учреждении культуры
«Специальная библиотека Кузбасса для незрячих и слабовидящих»**

1. Общие положения

1. Настоящее Положение определяет статус, задачи, функции, права и ответственность лица, назначаемого ответственным за эксплуатацию средств криптографической защиты информации (далее – ответственный за СКЗИ), в государственном казённом учреждении культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее – Организации).

2. Ответственный за СКЗИ назначается руководителем Организации.

3. Ответственный за СКЗИ осуществляет свою деятельность на основе настоящего Положения и подчиняется непосредственно руководителю Организации либо лицу, его замещающему.

5. Указания и поручения ответственного за СКЗИ в пределах его компетенции являются обязательными для исполнения всеми работниками, использующими СКЗИ.

6. В своей деятельности руководствуется: ФЗ-149, ФЗ-152, ФЗ-187, Приказом ФСТЭК №117, нормативными правовыми актами ФСБ России, иными документами, Политикой защиты информации, эксплуатационной документацией на СКЗИ, настоящим Положением.

2. Квалификационные требования

8. Ответственный за СКЗИ должен иметь высшее или среднее профессиональное образование. При наличии образования по направлению, не относящемуся к ИТ или ИБ, рекомендуется пройти обучение по программе профессиональной переподготовки в области защиты информации с использованием СКЗИ.

9. Ответственный за СКЗИ должен обладать знаниями: нормативных правовых актов в области СКЗИ; требований ФСБ и ФСТЭК к установке, настройке и эксплуатации сертифицированных СКЗИ; порядка учёта, хранения и обращения с ключевыми документами; правил ведения документации; порядка действий при компрометации ключей; принципов функционирования применяемых СКЗИ.

10. Ответственный за СКЗИ должен обладать умениями: установки, настройки и эксплуатации сертифицированных СКЗИ; ведения учёта СКЗИ, ключевых документов, носителей; проведения инструктажа пользователей;

оформления заключений о допуске; организации контроля соблюдения условий хранения; реагирования на компрометацию.

3. Трудовые обязанности ответственного лица

11. Ответственный за СКЗИ выполняет следующие функции:

- а) организует и обеспечивает эксплуатацию СКЗИ в соответствии с требованиями;
- б) разрабатывает и актуализирует локальные нормативные акты по вопросам применения, учёта и хранения СКЗИ, ключевых документов;
- в) осуществляет установку, настройку и сопровождение СКЗИ во взаимодействии с администратором безопасности и системным администратором;
- г) ведёт учёт СКЗИ, ключевых документов и носителей ключевой информации в установленных журналах и учётных формах;
- д) организует хранение СКЗИ, ключевых документов и носителей в условиях, исключающих несанкционированный доступ, утрату или повреждение;
- е) проводит инструктаж пользователей, допускаемых к работе с СКЗИ, по правилам эксплуатации и обеспечения сохранности ключевой информации;
- ё) оформляет заключения о возможности допуска пользователей к самостоятельной работе с СКЗИ, а также о возможности эксплуатации СКЗИ;
- ж) осуществляет контроль за соблюдением пользователями правил эксплуатации СКЗИ, хранения и использования ключевых документов;
- з) организует проведение проверок наличия и состояния СКЗИ, ключевых документов, условий их хранения;
- и) принимает меры по оперативной замене ключевых документов в случаях их компрометации, утраты или истечения срока действия, информирует ответственного за организацию защиты информации, администратора безопасности и руководителя;
- к) организует взаимодействие с организациями – разработчиками (поставщиками) СКЗИ по вопросам эксплуатации, замены, обновления;
- л) обеспечивает применение сертифицированных СКЗИ в соответствии с требованиями ФСБ и ФСТЭК;
- м) подготавливает отчёты о состоянии эксплуатации СКЗИ для ответственного за организацию защиты информации и руководителя.

4. Права ответственного лица

12. Ответственный за СКЗИ вправе:

- а) запрашивать и получать информацию, необходимую для выполнения функций;
- б) проводить проверки соблюдения правил эксплуатации СКЗИ, условий хранения и использования ключевых документов;

- в) давать обязательные для исполнения указания по вопросам эксплуатации СКЗИ;
- г) требовать от пользователей соблюдения правил работы с СКЗИ и ключевыми документами;
- д) отказывать в допуске к работе с СКЗИ при несоответствии квалификации или нарушении условий (с уведомлением ответственного за организацию защиты информации и администратора безопасности);
- е) инициировать замену или обновление СКЗИ, а также замену ключевых документов;
- ё) приостанавливать эксплуатацию СКЗИ при выявлении нарушений или признаков компрометации (с уведомлением ответственного за организацию защиты информации и администратора безопасности);
- ж) вносить предложения о совершенствовании порядка эксплуатации СКЗИ, приобретении новых средств, повышении уровня защиты ключевой информации;
- з) привлекать (по согласованию с ответственным за организацию защиты информации) лицензиатов ФСБ России для выполнения отдельных работ.

5. Ответственность

13. Ответственный за СКЗИ в соответствии с законодательством несёт ответственность:

- а) за неисполнение или ненадлежащее исполнение возложенных обязанностей;
- б) за нарушение установленного порядка учёта, хранения и эксплуатации СКЗИ и ключевых документов;
- в) за непринятие мер по замене ключевых документов в установленные сроки или при их компрометации;
- г) за нарушения в настройке СКЗИ, повлёкшие снижение уровня защищённости;
- д) за разглашение сведений о СКЗИ, ключевых документах и организации их использования;
- е) за несвоевременное информирование о нарушениях, компрометации ключей или инцидентах;
- ё) за нарушение требований по применению сертифицированных СКЗИ.

14. Нарушение ответственным за СКЗИ требований влечёт дисциплинарную, административную или уголовную ответственность.

**Положение об ответственном
за техническое обслуживание информационных систем
государственного казённого учреждения культуры
«Специальная библиотека Кузбасса для незрячих и слабовидящих»**

1. Общие положения

1. Настоящее Положение определяет статус, задачи, функции, права и ответственность лица, назначаемого ответственным за техническое обслуживание информационных систем (далее – администратор системы), в государственном казённом учреждении культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее – Организации).

2. Администратор системы назначается руководителем Организации.

3. Администратор системы осуществляет свою деятельность на основе настоящего Положения и подчиняется и подчиняется непосредственно руководителю Организации либо лицу, его замещающему.

4. Указания и поручения администратора системы в пределах его компетенции являются обязательными для исполнения пользователями ИС.

5. В своей деятельности руководствуется: ФЗ-149, ФЗ-152, ФЗ-187, Приказом ФСТЭК №117, иными нормативными и методическими документами, национальными стандартами, Политикой защиты информации, эксплуатационной документацией на программные, программно-аппаратные и технические средства, настоящим Положением.

2. Квалификационные требования

6. Администратор системы должен иметь высшее или среднее профессиональное образование (желательно в области ИТ). При наличии образования по направлению, не относящемуся к ИТ, рекомендуется пройти обучение по программе профессиональной переподготовки в области ИТ или защиты информации.

7. Администратор системы должен обладать знаниями: принципов построения и функционирования ОС, СУБД, сетевых протоколов, аппаратного обеспечения; порядка установки, настройки и сопровождения серверного и пользовательского оборудования, системного и прикладного ПО; методов резервного копирования и восстановления данных; основных угроз безопасности информации; правил безопасной конфигурации; порядка взаимодействия с администратором безопасности.

8. Администратор системы должен обладать умениями: установки, настройки и сопровождения программных и программно-аппаратных средств ИС; администрирования ОС и сетевого оборудования; проведения

инвентаризации активов; обеспечения резервного копирования и восстановления данных; управления обновлениями (совместно с администратором безопасности); выявления и устранения технических неисправностей.

3. Трудовые обязанности ответственного лица

8. Администратор системы выполняет следующие функции:

а) обеспечивает техническую эксплуатацию программных, программно-аппаратных и технических средств ИС, их работоспособность и устойчивое функционирование;

б) осуществляет установку, настройку и сопровождение ОС, СУБД, прикладного ПО, сетевого и серверного оборудования;

в) проводит инвентаризацию активов ИС, ведёт учёт в установленных формах;

г) обеспечивает выполнение процедур резервного копирования информации, конфигураций и ПО, контролирует целостность и сохранность резервных копий, участвует в проведении тестового восстановления;

д) совместно с администратором безопасности участвует в управлении обновлениями ПО: обеспечивает тестирование обновлений (при наличии тестовой среды), установку обновлений в соответствии с установленными правилами;

е) взаимодействует с администратором безопасности при настройке средств защиты, обеспечении соответствия конфигураций утверждённым эталонным образцам;

ё) выявляет и устраняет технические неисправности оборудования и ошибки в работе ПО, восстанавливает работоспособность ИС в установленные сроки;

ж) контролирует целостность программно-аппаратной среды, выявляет факты несанкционированного изменения конфигураций или установки ПО, информирует администратора безопасности и ответственного за организацию защиты информации;

з) предоставляет администратору безопасности информацию, необходимую для выявления и устранения уязвимостей, анализа событий безопасности, расследования инцидентов;

и) участвует в планировании и реализации мероприятий по модернизации технической инфраструктуры, обеспечению отказоустойчивости и масштабируемости;

к) обеспечивает техническую поддержку выполнения требований по устойчивости функционирования значимых объектов КИИ (при их наличии), участвует в реализации планов обеспечения непрерывности;

л) подготавливает отчёты о результатах технического обслуживания ИС для ответственного за организацию защиты информации и руководителя.

4. Права ответственного лица

9. Администратор системы вправе:

- а) запрашивать и получать от структурных подразделений и должностных лиц информацию, необходимую для выполнения функций;
- б) получать доступ к оборудованию, ПО и конфигурациям ИС в объёме, необходимом для выполнения обязанностей;
- в) вносить изменения в конфигурации технических средств и ПО в порядке, установленном локальными нормативными актами, с обязательным документированием изменений;
- г) требовать от пользователей соблюдения установленных правил работы с техническими средствами и ПО;
- д) приостанавливать эксплуатацию оборудования или ПО при выявлении угроз безопасности (с незамедлительным уведомлением администратора безопасности и ответственного за организацию защиты информации);
- е) инициировать проведение внеплановых проверок технического состояния оборудования, резервного копирования, целостности программной среды;
- ё) вносить предложения о модернизации технических средств, приобретении нового оборудования, повышении надёжности и отказоустойчивости.

5. Ответственность

10. Администратор системы в соответствии с законодательством несет ответственность:

- а) за неисполнение или ненадлежащее исполнение возложенных обязанностей;
- б) за несвоевременное или некачественное выполнение работ по техническому обслуживанию, приведшее к нарушению работоспособности ИС;
- в) за нарушения в настройке оборудования и ПО, повлёкшие снижение уровня защищённости или возникновение уязвимостей;
- г) за несоблюдение установленных процедур резервного копирования, повлёкшее утрату или невозможность восстановления данных;
- д) за несвоевременное информирование администратора безопасности и ответственного за организацию защиты информации о нарушениях, инцидентах, изменениях конфигураций;
- е) за нарушение требований по обеспечению устойчивости функционирования значимых объектов КИИ (при их наличии).

14. Нарушение администратором системы требований информационной безопасности влечёт дисциплинарную, административную или уголовную ответственность.

**Положение о пользователях информационных систем
государственного казённого учреждения культуры
«Специальная библиотека Кузбасса для незрячих и слабовидящих»**

1. Общие положения

1. Настоящее Положение определяет статус, задачи, функции, права и ответственность пользователей информационных систем (далее – пользователи), в государственном казённом учреждении культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее – Организации).

2. Пользователями являются работники Организации, а также иные лица, которым в установленном порядке предоставлен доступ к ИС для выполнения служебных (трудовых) обязанностей или в соответствии с договорными обязательствами.

3. Доступ пользователей к ИС предоставляется на основании приказа руководителя или уполномоченного им лица, а также оформленной в установленном порядке заявки.

4. Пользователи обязаны соблюдать требования законодательства в области защиты информации, Политики защиты информации, стандарта, иных локальных актов, а также правила работы в ИС.

6. В своей деятельности пользователи руководствуются: ФЗ-149, ФЗ-152, ФЗ-187, Приказом ФСТЭК №117, иными нормативными документами, Политикой защиты информации, настоящим Положением, эксплуатационной документацией.

2. Квалификационные требования

7. Пользователь должен быть ознакомлен с требованиями настоящего Положения и иных локальных актов, регламентирующих обработку информации и работу в ИС.

8. Пользователь обязан пройти вводный инструктаж по информационной безопасности до момента предоставления доступа к ИС.

9. Пользователь должен обладать знаниями и навыками: правил работы с учётными данными; порядка действий при выявлении признаков несанкционированного доступа; ответственности за нарушения; основных правил защиты информации, включая запрет на передачу учётных данных третьим лицам, несанкционированное копирование и распространение информации.

10. Пользователи, имеющие доступ к персональным данным или иной информации ограниченного доступа, дополнительно проходят инструктаж по особенностям работы с такими данными.

3. Трудовые обязанности пользователя

11. Пользователь обязан:

а) соблюдать требования нормативных правовых актов, Политики защиты информации, иных локальных актов, правил работы в ИС;

б) использовать ИС и содержащуюся в них информацию исключительно для выполнения служебных обязанностей, в соответствии с предоставленными правами доступа;

в) обеспечивать сохранность учётных данных (логинов, паролей, токенов, электронных ключей), не передавать их третьим лицам, не записывать пароли на бумажные носители, не хранить их в открытом виде;

г) незамедлительно информировать администратора безопасности или ответственного за организацию защиты информации, а также своего непосредственного руководителя о любых попытках несанкционированного доступа, подозрительных событиях, утрате или компрометации учётных данных, утрате носителей информации;

д) своевременно сообщать ответственному за организацию защиты информации или администратору безопасности об изменении своих персональных данных, должностных обязанностей, а также о прекращении необходимости использования ИС;

е) завершать работу в ИС по окончании рабочего дня, блокировать рабочую станцию при временном оставлении рабочего места;

ё) соблюдать правила обращения со съёмными носителями информации, не использовать несанкционированные носители для переноса информации, не выносить носители с информацией ограниченного доступа за пределы контролируемой зоны без разрешения;

ж) использовать только установленное и санкционированное ПО, не устанавливать самостоятельно программные средства без согласования с администратором безопасности;

з) соблюдать правила работы в сети Интернет, установленные в Организации, не использовать ИС в личных целях, не совершать действий, направленных на нарушение работы ИС или средств защиты;

и) проходить в установленные сроки инструктажи и обучение по вопросам ИБ, подтверждать ознакомление с локальными актами под подпись;

к) при прекращении трудовых отношений или истечении срока действия договора вернуть все выданные носители информации, токены, ключи электронной подписи и иные средства доступа.

4. Права пользователя

12. Пользователь вправе:

а) получать доступ к ИС и содержащейся в них информации в объёме, необходимом для выполнения трудовых обязанностей;

б) обращаться к администратору безопасности, ответственному за организацию защиты информации или непосредственному руководителю за разъяснениями по вопросам работы в ИС и соблюдения требований ИБ;

в) своевременно получать информацию об изменениях правил работы в ИС, о новых угрозах и способах защиты;

г) подавать заявки на предоставление, изменение или прекращение прав доступа в установленном порядке;

д) получать необходимые технические и программные средства для выполнения служебных обязанностей в соответствии с установленными правилами.

5. Ответственность

13. Пользователь в соответствии с законодательством несет ответственность:

а) за несоблюдение требований настоящего Положения, Политики защиты информации, иных локальных актов;

б) за нарушение правил обработки информации ограниченного доступа (конфиденциальной информации, персональных данных), включая её разглашение;

в) за передачу учётных данных третьим лицам, использование чужих учётных данных;

г) за несанкционированное изменение конфигураций программных и технических средств, установку несанкционированного ПО;

д) за несвоевременное информирование администратора безопасности или ответственного за организацию защиты информации о компрометации учётных данных, утрате носителей, инцидентах;

е) за использование ИС в целях, не связанных с исполнением служебных обязанностей, или в личных целях;

ё) за утрату носителей информации, токенов, ключей электронной подписи, повлёкшую возможность несанкционированного доступа.

14. Нарушение пользователем требований информационной безопасности влечёт дисциплинарную, административную или уголовную ответственность.