Приложение № 1

УТВЕРЖДАЮ:
Директор государственного казённого учреждения культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих»
_____ И. Ю. Тихонова
«24» декабря 2025 год

Политика информационной безопасности

государственного казённого учреждения культуры

«Специальная библиотека Кузбасса для незрячих и слабовидящих»

ОГЛАВЛЕНИЕ

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящая Политика информационной безопасности государственного казённого учреждения культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее – Политика) распространяется на все процессы и информационные системы государственного казённого учреждения культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих» (далее - Библиотека) и обязательна для применения всеми работниками и руководством Библиотеки.

1.2. Лица, осуществляющие разработку документов Библиотеки, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

2. НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей и информации, причиняющей вред их развитию и здоровью»;
- Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»;
- Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место.

Производственный процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Библиотеки.

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность (ИБ) – состояние защищённости интересов Библиотеки.

ИС – информационная система.

Информационный ресурс (актив) – всё, что имеет ценность и находится в распоряжении Библиотеки.

Инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могло привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Инцидент информационной безопасности – одно или серия нежелательных или

неожиданных событий ИБ, имеющих значительную вероятность нарушения производственных процессов или представляющих угрозу ИБ.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

ИМО – инновационно-методический отдел государственного казённого учреждения культуры «Специальная библиотека Кузбасса для незрячих и слабовидящих».

Политика – общие цели и указания, формально выраженные руководством Библиотеки.

ПО - программное обеспечение.

Риск – сочетание вероятности события и его последствий.

СКЗИ - средства криптографической защиты информации.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации.

ЭП – электронная цифровая подпись.

4. ЦЕЛЬ И ЗАДАЧИ

Цель настоящей Политики – защита информационных ресурсов Библиотеки от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, минимизация рисков ИБ.

Для достижения цели настоящей Политики обеспечивается решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИБ посторонних лиц;
- соответствие требованиям законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
- обеспечение непрерывности производственных процессов;
- достижение адекватности мер по защите от угроз ИБ;
- недопущение проникновения лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников Библиотеки;
- повышение деловой репутации и корпоративной культуры в Библиотеке.

5. СОДЕРЖАНИЕ ПОЛИТИКИ

5.1. Система управления ИБ.

Для достижения указанных цели и задач в Библиотеке внедрена СУИБ.

СУИБ включает процессы управления ИБ, персонал, ответственный за обеспечение и организацию управления ИБ, и комплект документированных политик и процедур.

СУИБ документирована в настоящей Политике, в правилах, процедурах, которые являются обязательными для всех работников Библиотеки в области действия СУИБ. Документированные требования СУИБ доводятся до сведения работников Библиотеки.

Средства управления ИБ внедряются по результатам проведения оценки рисков ИБ. Стоимость внедряемых средств управления ИБ не должна превышать возможный ущерб, возникающий при реализации угроз.

5.1.1. Структура документов.

В целях создания взаимосвязанной структуры нормативных документов Библиотеки в области обеспечения ИБ разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

- Политика информационной безопасности.
- Инструкции.
- Документы, подтверждающие исполнение нормативных актов верхних уровней.

Настоящая Политика является внутренним нормативным документом по ИБ **первого уровня**.

Документы **второго уровня** – это инструкции и прочие документы, описывающие действия работников Библиотеки по реализации документов первого и второго уровня.

Документы **третьего уровня** – это отчётные документы о выполнении требований документов верхних уровней.

5.1.2. Ответственность за обеспечение ИБ.

Для непосредственной организации и эффективного функционирования СУИБ в Библиотеке функции обеспечения ИБ возложены на ИМО, выполняя которые ИМО решает следующие задачи:

- определение требований к защите информации;
- организация мероприятий и координация работ всех структурных подразделений Библиотеки по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты;
- оказание методической помощи работникам Библиотеки в вопросах обеспечения ИБ;
- регулярная оценка и управление рисками ИБ в соответствии с установленными процедурами в области управления рисками;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
- обеспечение минимально необходимого доступа к информационным ресурсам, основываясь на требованиях производственных процессов;
- информирование, обучение работников Библиотеки в сфере ИБ;
- анализ инцидентов ИБ;
- сбор, накопление, систематизация и обработка информации по вопросам ИБ;
- обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для структурных подразделений Библиотеки.

Для решения задач, возложенных на ИМО, его сотрудники имеют следующие права:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей ИС в указанной области;
- получать информацию от пользователей ИС Библиотеки по любым аспектам применения информационных технологий в Библиотеке;
- участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
- участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
- контролировать деятельность пользователей Библиотеки по вопросам обеспечения ИБ;
- готовить предложения руководству Библиотеки по обеспечению требований ИБ.

5.2. ОБЪЕКТЫ ЗАЩИТЫ

5.2.1. Ответственность за ресурсы.

На основе информации обо всех ресурсах Библиотеки, выявленных и оценённых, с точки зрения их важности, в Библиотеке реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

Типы ресурсов Библиотеки:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Библиотеки;
- открыто распространяемая информация, необходимая для работы Библиотеки, независимо от формы и вида её представления;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Для каждого ресурса Библиотеки назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.

5.2.2. Классификация информации.

Все информационные ресурсы Библиотеки, подлежащие защите, классифицированы в соответствии с их важностью и степенью доступа. Классификация информации документирована и утверждена руководством Библиотеки.

Классификация информации проводится владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация пересматривается для поддержания актуальности её соответствия с категорией ресурса.

5.3. БЕЗОПАСТНОСТЬ ПЕРСОНАЛА

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с настоящей Политикой, доведены до работников Библиотеки (общие обязанности по реализации и поддержке политики безопасности и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью).

5.3.1. Ответственность руководства Библиотекой.

Руководство Библиотекой требует от работников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Библиотеке настоящей Политикой и иными процедурами.

Уполномоченные руководством Библиотеки работники имеют право в установленном порядке, без уведомления, производить проверки:

- выполнения действующих инструкций по вопросам ИБ;
- данных, находящихся на носителях информации;
- порядка использования работниками Библиотеки информационных ресурсов;
- содержания служебной переписки.

5.3.2. Обучение ИБ.

Все работники Библиотеки проходят периодическую подготовку в области политики и процедур ИБ, принятых в Библиотеке.

5.3.3. Завершение или изменения трудовых отношений.

При увольнении все предоставленные работнику Библиотеки права доступа к ресурсам ИС удаляются работниками ИМО. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых трудовых отношениях.

5.4. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

5.4.1. Защищённые области.

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Библиотеки, размещены в защищённых областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации. Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, шкафами, оборудованными замком.

5.4.2. Области общего доступа.

Места доступа, через которые неавторизованные лица могут попасть в помещения Библиотеки, контролируются видеофиксацией, с целью предотвращения несанкционированного доступа.

5.4.3. Вспомогательные службы.

Вспомогательные службы (электропитание, отопление, вентиляция и кондиционирование воздуха) обеспечивают гарантированную и устойчивую работоспособность компонентов ИС Библиотеки.

5.4.4. Утилизация или повторное использование оборудования.

С носителей информации, которыми укомплектовано утилизируемое оборудование, удаляются все конфиденциальные данные и лицензионное ПО. Отсутствие защищаемой информации на носителях проверяется ИМО.

5.4.5. Перемещение имущества.

Оборудование, информация или ПО перемещаются за пределы Библиотеки при наличии письменного разрешения руководства Библиотеки.

5.5. КОНТРОЛЬ ДОСТУПА

Основными пользователями информации в ИС Библиотеки являются сотрудники структурных подразделений Библиотеки. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Каждому пользователю, допущенному к работе с конкретным информационным активом Библиотеки, сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он регистрируется и работает с информационным активом.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИС, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИС).

Запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей.

Регистрируемые учётные записи подразделяются на:

- пользователя – для работы в системе;
- администратора – для администраторов ИМО.

Процедуры регистрации и блокирования учётных записей пользователей применяются с соблюдением следующих правил:

- регистрация и блокирование учётных записей выполняется ИМО;
- уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
- обеспечение создания и поддержания списка всех пользователей, зарегистрированных для работы с информационными ресурсами или сервисом;
- немедленное удаление или блокирование прав доступа пользователей, сменивших

должность, форму занятости или уволившихся из Библиотеки;

- аудит учётных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
- обеспечение того, чтобы учётные записи пользователей не были доступны другим пользователям;
- обеспечение возможности предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путём суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

5.5.1. Управление паролями.

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей контролируется посредством официальной процедуры, отвечающей следующим требованиям:

- при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;
- временные пароли назначаются пользователю только после его идентификации;
- недопущение передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли хранятся в электронном виде только в защищенной форме;
- назначенные производителем ПО пароли изменяются сразу после завершения инсталляции ПО;
- установлены требования к длине пароля, набору символов и числу попыток ввода (см. пункт 5.5.3 настоящей Политики);
- пароли пользователей изменяются не реже одного раза в 90 дней.

5.5.2. Контроль прав доступа.

Контроль над выполнением процедур управления доступом пользователей включает:

- проверку подлинности пользователей перед сменой паролей;
- немедленное блокирование прав доступа при увольнении работников Библиотеки;
- включение учётных записей, используемых поставщиками для удалённой поддержки, только на время выполнения работ;
- отслеживание удалённых учётных записей, используемых поставщиками, во время работ;
- ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;
- использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;
- разрешение запросов и прямого доступа к базам данных только для администраторов баз данных.

5.5.3. Использование паролей.

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых работнику Библиотеки предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) работником информации.

Не допускается использование различными пользователями одних и тех же учётных данных.

Первоначальное значение пароля учетной записи пользователя устанавливает администратор безопасности.

Личные пароли устанавливаются первый раз сотрудниками ИМО. После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля должны присутствовать три из четырёх видов символов:
  - латинские буквы в верхнем регистре;
  - латинские буквы в нижнем регистре;
  - цифры;
  - один специальный символ (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);
- пароль не должен содержать легко вычисляемые сочетания символов, например,
  - имена, фамилии, номера телефонов, даты;
  - последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);
  - общепринятые сокращения («USER», «TEST» и т.п.);
  - компьютерный термин, команда, наименование компаний, web-сайтов, аппаратного или программного обеспечения;
  - что-либо из вышеперечисленного в обратном написании;
  - что-либо из вышеперечисленного с добавлением цифр в начале или в конце;
- при смене пароля значение нового пароля должно отличаться от предыдущего не менее чем в 4 позициях;
- для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

Работнику Библиотеки запрещается:

- сообщать свой пароль кому-либо;
- указывать пароль в сообщениях электронной почты;
- хранить пароли, записанные на бумаге, в легко доступном месте;
- использовать тот же самый пароль, что и для других систем (например, домашний интернет-провайдер, бесплатная электронная почта, форумы и т.п.);
- использовать один и тот же пароль для доступа к различным корпоративным ИС.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место, пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Работник Библиотеки обязан:

- в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации сотруднику ИМО;
- немедленно сообщить сотруднику ИМО в случае получения от кого-либо просьбы сообщить пароль;
- менять пароль каждые 90 дней;
- менять пароль по требованию администратора ИБ.

После 20 неудачных попыток ввода пароля учётная запись блокируется на 10 минут. При систематической блокировке учётной записи работником Библиотеки (более 3 раз) оповещается администратор ИБ.

Библиотека вправе осуществлять периодическую проверку стойкости паролей пользователей, используемых работниками Библиотеки для доступа к ИС, и принимать меры дисциплинарного характера к работникам Библиотеки, нарушающим положения настоящей Политики.

5.5.4. Пользовательское оборудование, оставляемое без присмотра.

Работники Библиотеки осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, о своих обязанностях по обеспечению этой защиты и обеспечивают необходимую защиту оборудования, остающегося без присмотра.

5.5.5. Политика чистого стола.

Работники Библиотеки обязаны:

- документы и носители с конфиденциальной информацией убирать в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места;

- компьютеры оставлять в состоянии выполненного выхода из системы, когда они находятся без присмотра;

- документы, содержащие конфиденциальную информацию, изымать из печатающих устройств немедленно;

- для утилизации конфиденциальных документов использовать уничтожитель бумаги;

- в конце рабочего дня привести в порядок письменный стол и убрать все документы в запираемый шкаф или сейф; в случае длительного отсутствия на рабочем месте запирать на замки все шкафы и сейфы.

5.5.6. Мобильное компьютерное оборудование.

При использовании мобильных средств (ноутбуков, планшетов и мобильных телефонов) соблюдаются особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Библиотеке. Принята официальная политика, учитывающая риск, связанный с использованием мобильных компьютеров, в частности, с работой в незащищённой среде.

5.6. ПОЛИТИКА ДОПУСТИМОГ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Общие обязанности работников Библиотеки:

- при работе с ПО руководствоваться нормативной документацией (руководством пользователя);
- обращаться в ИМО по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), за необходимой методической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;
- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
- минимизировать вывод на печать обрабатываемой информации.

5.6.1. Использование ПО.

На АРМ Библиотеки допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

Запрещено незаконное хранение на жестких дисках информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры и т.д.).

Решение об установке ПО и реализации других задач принимает заведующий ИМО.

Документы, подтверждающие покупку ПО, хранятся в бухгалтерии Библиотеки на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в ИМО.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ Библиотеки. Указанные работы и работы по установке, регистрации и активации приобретённого лицензионного ПО выполняются сотрудниками ИМО.

Сведения о вновь приобретённом ПО должны быть внесены в перечень разрешённого программного обеспечения.

5.6.2. Использование АРМ и ИС.

К работе в ИС Библиотеки допускаются лица, назначенные на соответствующую должность. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Библиотеке, возложена на ИМО.

Каждый сотрудник Библиотеки, обеспеченный АРМ, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для

хранения рабочих файлов.

АРМ Библиотеки имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется ИМО.

В случае обнаружения неисправности компьютерного оборудования или ПО, сотрудник Библиотеки делает заявку в ИМО.

Сотрудники ИМО осуществляют контроль над установленным на компьютере ПО и принимают меры по ограничению возможностей несанкционированной установки программ.

При работе в ИС Библиотеки сотрудник Библиотеки обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов Библиотеки;
- использовать ИС и АРМ Библиотеки исключительно для выполнения своих служебных обязанностей;
- ставить в известность программиста ИМО о любых фактах нарушения требований ИБ;
- ставить в известность программиста ИМО о любых фактах сбоев ПО, некорректного завершения значимых операций, повреждения технических средств;
- предоставлять АРМ программисту ИМО для контроля;
- при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;

При использовании ИС Библиотеки запрещено:

- использовать АРМ и ИС в личных целях;
- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать:
  - конфиденциальную информацию (за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с ИМО);
  - информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
  - угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Библиотеки;
- предоставлять сотрудникам Библиотеки (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Библиотеки;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;
- использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

Информация о посещаемых развлекательных ресурсах отслеживается ИМО и представляется руководителям структурных подразделений и руководству Библиотеки.

Электронные сообщения и документы в электронном виде, передаваемые посредством ИС Библиотеки, подлежат обязательной проверке на отсутствие вредоносного ПО.

5.6.3. Использование ресурсов локальной сети.

Для выполнения служебных обязанностей каждый сотрудник Библиотеки обеспечивается доступом к сетевым папкам хранения на дисках серверов Библиотеки.

5.6.4. Обработка конфиденциальной информации.

При обработке конфиденциальной информации сотрудники Библиотеки обязаны:

- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера

сразу по окончании печати;

- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;
- не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD-диски, Flash-устройства и пр.), распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

5.6.5. Использование электронной почты.

Электронная почта используется для обмена в рамках ИС Библиотеки и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде. Для обеспечения функционирования электронной почты допускается применение ПО, входящего в реестр разрешённого к использованию ПО.

При работе с корпоративной электронной почтой Библиотеки сотрудники Библиотеки учитывают, что электронная почта не является средством гарантированной доставки отправленного сообщения до адресата и средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

Организацией и обеспечением порядка работы электронной почты в Библиотеке занимается ИМО.

Каждый сотрудник Библиотеки получает почтовый адрес, вида: name@домен.ru в домене Библиотеки. Адрес электронной почты выдаётся сотрудником ИМО при начальной регистрации пользователя в домене Библиотеки.

Корпоративная электронная почта Библиотеки предназначена для использования в служебных целях. Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Библиотеке. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты, принадлежат Библиотеке и являются неотъемлемой частью ее производственного процесса.

Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Библиотеки либо удалены программистом ИМО.

Пользователям корпоративной электронной почты Библиотеки запрещено вести частную переписку (переписку, не связанную с исполнением сотрудником Библиотеки своих должностных обязанностей). Использование сотрудниками Библиотеки корпоративной электронной почты Библиотеки для частной переписки является нарушением трудовой дисциплины Библиотеки. Подписывая ознакомление с настоящей Политикой, сотрудники Библиотеки дают согласие на ознакомление и иное использование в интересах Библиотеки их переписки, осуществляемой с использованием корпоративной электронной почты Библиотеки, и соглашается с тем, что любое использование их переписки, осуществляемой с использованием корпоративной электронной почты Библиотеки, не рассматривается как нарушение тайны связи.

Каждый сотрудник Библиотеки имеет право на просмотр, иное использование в интересах Библиотеки сообщений корпоративной электронной почты Библиотеки, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес.

Использование сообщений корпоративной электронной почты Библиотеки осуществляется уполномоченными сотрудниками Библиотеки в соответствии с их функциями, определёнными в данной Политике и в иных локальных нормативных актах Библиотеки. Просмотр и иное использование сообщений электронной почты в интересах Библиотеки осуществляется сотрудниками Библиотеки в целях обеспечения защиты конфиденциальных сведений, обеспечения нормальной работоспособности системы электронной почты, в рамках обслуживания сервисов электронной почты, при выполнении ручной пересылки сообщений, приходящих на корпоративные электронные адреса Библиотеки сотрудникам или группам сотрудников, а также по мотивированным запросам

прямых или непосредственных руководителей любых сотрудников, чью почту необходимо использовать в интересах Библиотеки.

Использование сообщений корпоративной электронной почты в интересах Библиотеки, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.

Исходящие электронные сообщения сотрудников Библиотеки содержат поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

Формат подписи отправителя:

С уважением,
<Фамилия, имя, отчество>
<Должность>
<Структурное подразделение>
<Наименование учреждения>
<Адрес>
<номера контактов: телефон, мессенджеры, адреса электронной почты>
<сайт Библиотеки>

В случае получения служебного сообщения о невозможности доставки сообщения адресату или получения извещения от адресата о том, что он не получил отправленное ему сообщение, необходимо связаться с сотрудником ИМО.

Отказ от дальнейшего предоставления сотруднику Библиотеки услуг электронной почты может быть вызван нарушениями требований настоящей Политики.

Прекращение предоставления сотруднику Библиотеки услуг электронной почты наступает при прекращении действия трудового договора (контракта) сотрудника.

5.6.3. Работа в сети.

Доступ к сети Интернет предоставляется сотрудникам Библиотеки исключительно в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

Для доступа сотрудников Библиотеки к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

При использовании сети Интернет сотрудники Библиотеки соблюдают требования настоящей Политики, ставят в известность отдел ИМО о любых фактах нарушения требований настоящей Политики.

При использовании сети Интернет сотрудникам Библиотеки запрещено:

- использовать предоставленный Библиотекой доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Библиотеки;
- публиковать, загружать и распространять материалы, содержащие:

○ конфиденциальную информацию, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным;
○ угрожающую, клеветническую, непристойную информацию;
○ вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
○ фальсифицировать свой IP-адрес, а также прочую служебную информацию.

Библиотека блокирует или ограничивает доступ сотрудников к Интернет-ресурсам, содержание которых не имеет отношения к исполнению ими служебных обязанностей, а

также к ресурсам, содержание и направленность которых запрещены законодательством.

Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

5.6.4. Использование носителей информации.

Под использованием носителей информации в ИС Библиотеки понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и носителями информации.

К предоставленным Библиотекой носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. При использовании предоставленных Библиотекой носителей информации, сотрудники Библиотеки обязаны:

- соблюдать требования настоящей Политики;
- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность программиста ИМО о любых фактах нарушения требований настоящей Политики;
- эксплуатировать и транспортировать носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность носителей информации всеми разумными способами;
- извещать программиста ИМО о фактах утраты (кражи) носителей информации.

При использовании предоставленных сотруднику Библиотеки носителей информации запрещено использовать носители информации в личных целях, передавать носители информации другим лицам (за исключением программиста ИМО), оставлять носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём\передача информации), инициированное сотрудником Библиотеки между ИС и неучтёнными (личными) мобильным и устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговорённых с администраторами ИС заранее). Библиотека блокирует или ограничивает использование таких устройств и носителей информации.

Информация, хранящаяся на предоставляемых Библиотекой носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае увольнения, предоставленные сотруднику Библиотеки носители информации изымаются.

5.6.5. Защита от вредоносного ПО.

ИМО регулярно проверяет сетевые ресурсы Библиотеки антивирусным ПО и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудники Библиотеки незамедлительно оповещают об этом ИМО. После чего программист ИМО проводит внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники Библиотеки:

- останавливают работу и немедленно ставят в известность о факте обнаружения заражения своего руководителя и ИМО, владельца файла и смежные подразделения Библиотеки, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов проводят анализ необходимости дальнейшего их использования.

Для предупреждения вирусного заражения сотрудники Библиотеки:

- не открывают файлы и не выполняют макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя, удаляют подозрительные вложения, не открывая их, очищают корзину, где хранятся удаленные сообщения;
- удаляют спам, рекламу и другие бесполезные сообщения;
- не загружают файлы и ПО из подозрительных или неизвестных источников;
- периодически резервируют важные данные и системную конфигурацию, хранят резервные копии в безопасном месте.

5.7. ПРИОБРЕТЕНИЕ, РАЗРАБОТКА И ОБСЛУЖИВАНИЕ ИС

5.7.1. Требования безопасности для ИС.

При описании требований к созданию новых ИС или к усовершенствованию существующих учитывается потребность в средствах обеспечения их безопасности. Требования к безопасности и средства защиты должны соответствовать ценности используемых информационных ресурсов и потенциальному ущербу для Библиотеки в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками. Системные требования к ИБ и процессам, обеспечивающим защиту информации, рассматриваются на ранних стадиях проектирования ИС.

5.6.1. Корректная обработка информации.

Данные, вводимые в прикладные системы, проверяются в целях гарантии их правильности и соответствия поставленной задаче.

5.6.2. Криптографические средства.

Поступающие в Библиотеку СКЗИ учитываются в журнале поэкземплярного учёта СКЗИ. В Библиотеке осуществляется управление ключами для эффективного применения криптографических методов, в целях недопущения компрометации или потери криптографических ключей, что может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Все ключи защищены от изменения, утери и уничтожения. Секретные и закрытые ключи защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей защищено физически.

Соглашения с внешними поставщиками криптографических услуг (удостоверяющими центрами) об уровне предоставляемого сервиса охватывают вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Криптографические системы и методы используются для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

5.6.2.1. Требований по обеспечению ИБ при использовании СКЗИ.

Шифрование – это криптографический метод, который используется для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ поставляются разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Библиотеки и включает:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;
- порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

При использовании шифрования в ИС Библиотеки применяются утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

5.6.2.2. Электронные подписи.

ЭП обеспечивают защиту аутентификации и целостности электронных документов.

ЭП применяются для любой формы документа, обрабатываемого электронным способом. ЭП реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

В Библиотеке обеспечена конфиденциальность личных ключей, которые хранятся в секрете в целях недопущения фальсификации подписей владельцев ключей. Защита целостности открытого ключа обеспечивается при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, отличаются от тех, которые используются для шифрования.

При использовании ЭП учитываются требования законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

5.6.2.3. Управление ключами.

Управление криптографическими ключами важно для эффективного использования криптографических средств, т.к. компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. В Библиотеке применяется система защиты для обеспечения использования в ИС Библиотеки криптографических методов в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который храниться в секрете). Методы с открытыми ключами используются для шифрования и для генерации цифровых подписей.

Ключи защищены от изменения и разрушения; секретным и личным ключам обеспечена защита от неавторизованного раскрытия с использованием криптографических методов. Физическая защита применяется для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Для безопасного взаимодействия с внешними пользователями ИС Библиотеки используются электронные сертификаты из утверждённого списка сертифицированных центров.

Секретные ключи пользователей хранятся аналогично хранению паролей.

О любом подозрении на компрометацию секретного ключа пользователь немедленно сообщает в ИМО.

Система обеспечения безопасности использования ключей основывается на согласовании способов, процедур и безопасных методов для:

- генерации ключей при использовании различных криптографических систем и приложений;
- генерации и получения сертификатов открытых ключей;
- рассылки ключей, предназначенных пользователям, включая инструкции по их активации при получении;
- хранения ключей (при наличии инструкции авторизованным пользователям для получения доступа к ключам);
- смены или обновления ключей, включая правила порядка и сроков смены ключей;
- порядка действий в отношении скомпрометированных ключей;
- аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из Библиотеки (в этом случае ключи архивируются);
- восстановления утерянных или испорченных ключей, для рассекречивания зашифрованной информации;
- архивирования и резервного копирования ключей;
- разрушения ключей;
- регистрация ключей и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации ключей определяются даты начала и конца действия, чтобы их можно было использовать лишь в течении ограниченного периода времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

В Библиотеке предусмотрено наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованном виде для доказательств в суде.

Соглашения с внешними поставщиками криптографических услуг (удостоверяющими центрами) об уровне предоставляемого сервиса охватывают вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

5.6.3. Безопасность системных файлов.

Для минимизации риска повреждения ИС в Библиотеке обеспечен контроль над внедрением ПО в рабочих системах. Тестовые данные находятся под контролем и защитой. Для испытаний используются значительные объёмы тестовых данных, максимально близко соответствующие рабочим данным. В рамках испытаний не используются рабочие базы данных, содержащие конфиденциальную информацию (в случае их использования конфиденциальные данные удаляются или изменяются).

5.8. СОБЛЮДЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА

Значимые требования, установленные законодательством, подзаконными актами и договорными отношениями, подход Библиотеки к обеспечению соответствия этим требованиям определены, документированы и поддерживаются в актуальном состоянии.

В Библиотеке соблюдается регламентированный процесс, предупреждающий нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, от стадии сбора и ввода данных до их хранения.

В Библиотеке внедрены процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, по использованию лицензионного ПО.

Важная документация Библиотеки защищена от утери, уничтожения и фальсификации. Система хранения и обработки обеспечивает идентификацию записей и их периода хранения в соответствии с требованиями законодательства и нормативных актов, имеет возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Библиотеке.

Криптографические средства используются в соответствии с имеющимися соглашениями, законодательными и нормативными актами.

6. ОТВЕТСТВЕННОСТЬ

Директор Библиотеки определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, осуществляет общее руководство обеспечением ИБ Библиотеки.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Библиотеки возложена на ИМО.

Руководители структурных подразделений Библиотеки несут прямую ответственность за реализацию настоящей Политики и её соблюдение подчиненными работниками.

Работники Библиотеки несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать о выявленных нарушениях в области ИБ в ИМО.

Руководство Библиотекой проводит совещания по проблемам обеспечения ИБ с целью формирования указаний по этому вопросу, осуществления контроля их выполнения, оказания административной поддержки инициативам по обеспечению ИБ.

Нарушение требований нормативных актов Библиотеки по обеспечению ИБ является чрезвычайным происшествием и служит поводом и основанием для проведения служебного расследования.

7. КОНТРОЛЬ И ПЕРЕСМОТР

Общий контроль состояния ИБ Библиотеки осуществляется директором Библиотеки.

Текущий контроль соблюдения настоящей Политики осуществляет ИМО путём проведения мониторинга инцидентов ИБ Библиотеки, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

ИМО 1 раз в 3 года пересматривает положения настоящей Политики. Изменения и дополнения утверждаются директором Библиотеки в установленном порядке.