Тип работы: Курсовая работа

Предмет: Библиотековедение

Содержание

ВВЕДЕНИЕ
Информация – это, прежде всего, ресурс, грамотное применение которого может как привести к успеху, так и стать причиной крупной неудачи. Исходя из этого важной задачей на современном этапе представляется сохранение и защита информации. Сегодня объём информационных ресурсов постоянно возрастает. Бумажные носители информации уже не могут в полной мере выполнять свои функции и постепенно вытесняются электронными носителями, информация на которых более подвержена утрате. В результате более актуальной становится проблема конфиденциальности информации. Таким образом, информации требуется защита и обеспечение безопасности.
Современные библиотеки, главная функция которых заключается в обеспечении пользователей информацией, обязаны обеспечить для читателей безопасное использование данной информации.

При этом пользователи библиотек являются сразу и основным субъектом библиотечного обслуживания, и дополнительными источником угрозы для информационных ресурсов библиотеки, размещённых как на бумажных, так и на электронных носителях информации.
В связи с этим от современных библиотек требуется принятие и исполнение решений по обеспечению должного хранения и защиты хранящейся в библиотеке информации.
Защита информации в библиотеках имеет 3 важных аспекта. Во-первых, это особенности библиотечного учреждения как субъекта защиты информации, которые обусловлены его характером библиотечной деятельности и функциональной спецификой данного учреждения культуры.
ГЛАВА I. АНАЛИЗ УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИБЛИОТЕКАХ
1.1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИБЛИОТЕК РОССИИ
В настоящее время возрастает значение разработки и внедрения инструментов и средств обеспечения информационной безопасности.
Информационная безопасность (ИБ) представляет собой «состояние защищённости национальных интересов России в информационной среде, обусловленных совокупностью сбалансированных интересов индивида, общества и государства» [24, с. 27].
Обеспечение безопасности информационных ресурсов (ИР), содержащихся в российских библиотеках (традиционных, магнитных и электронных), следует рассматривать как важнейший вопрос национальной безопасности России, связанный с Доктриной информационной безопасности РФ [1].
К объектам информационной безопасности в библиотечной среде специалисты относят права и свободы гражданина России, материальные и духовные ценности общества.
Информационная безопасность библиотек рассматривается, в первую очередь, с позиции доступности

информации. Выделяют общедоступную, конфиденциальную информацию (ограниченного доступа) и информацию, образующую государственную тайну (закрытая информация) [8].
Общедоступная информация предоставляется неограниченно и может свободно передаваться, тиражироваться и распространяться, если она не запрещена законом. Как раз общедоступная информация и выступает объектом накопления и хранения в библиотеках.
Информационная безопасность – многогранное понятие, которое не ограничивается только защитой информации. Здесь следует принимать во внимание как интересы субъектов информационных отношений, так и механизмы защиты данных интересов.
Интересы субъектов информационных отношений делятся на 3 вида:
1) доступность (возможность за короткое время получить необходимую информацию);
2) целостность (актуальность информации, её защищенность от разрушения и несанкционированного изменения);
3) конфиденциальность (защита от несанкционированного ознакомления) [11, с. 47].
Защита интересов субъектов информационных отношений включает меры следующего характера:

1) законодательные (нормативно-правовые акты, стандарты и др.);
2) административные (действия, предпринимаемые руководством);
3) процедурные (конкретные меры безопасности);
4) программно-технические (технические меры) [19, с. 111].
Законодательство об информационной безопасности включает нормы Конституции РФ, и иных правовых актов, закрепляющих юридические основы безопасности гражданина, общества и государства. К ключевым НПА в библиотечной сфере следует отнести: Доктрина информационной безопасности Российской Федерации [1], ФЗ «О библиотечном деле» [2], ФЗ «Об информации, информационных технологиях и о защите информации» [3], Постановление Правительства РФ «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну…» [4], Приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [5], ГОСТ Р 50922-2006. «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» [6].

1.2. СУЩНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ В БИБЛИОТЕКАХ

Понятие защиты информации содержится в ГОСТ Р 50922-2006. «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения». Согласно этому документу защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [6].
Объектом защиты информации выступает сама информация либо носитель информации, либо информационный процесс, которые нужно защищать согласно цели защиты информации.
Защита информации обеспечивается:
1) предотвращением несанкционированного доступа к информации и (или) передачи её лицам, не обладающим правами на доступ к информации;
2) своевременным обнаружением фактов несанкционированного доступа к информации;
3) предупреждением возможности негативных последствий нарушения порядка доступа к информации;
4) недопущением воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5) возможностью незамедлительного восстановления информации, изменённой либо уничтоженной в результате несанкционированного доступа;
6) непрерывным контролем за обеспечением должного уровня защищённости информации [20, с. 16].
Современные подходы к защите информации обладают следующей спецификой:

1. Системный подход к разработке и построению систем защиты информации, подразумевающий разумную интеграцию программных, организационных, физических и аппаратных характеристик, применяемых на каждом этапе обработки информации.
2. Принцип непрерывного совершенствования системы информационной защиты в соответствии с возрастанием рисков утечки данных. Этот процесс постоянен и состоит в применении методов и инструментов совершенствования систем ИБ, непрерывном контроле, выявлении слабых мест системы и

потенциальных каналов утечки данных.
3. Обеспечение надёжности систем защиты информации, иными словами, контроль степени надёжности при отказе системы, появлении сбоев, взломе и аппаратных и программных ошибках.
4. Постоянный контроль за работой системы информационной защиты, совершенствование инструментов и методов контроля за функционированием механизмов защиты информации.
5. Совершенствование методов борьбы с вредоносными программами, спамом и вирусами.
6. Оптимизация расходов на разработку и эксплуатацию систем информационной защиты, проявляющаяся в экономической целесообразности использования систем ИБ [35, с. 64].

ГЛАВА II. СПОСОБЫ ЗАЩИТЫ ПЕЧАТНОЙ ИНФОРМАЦИИ БИБЛИОТЕЧНЫХ ФОНДОВ

2.1. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕЧАТНЫХ ИЗДАНИЙ В БИБЛИОТЕКАХ

Библиотеки получают, хранят и предоставляют в бесплатное пользование документы различных типов. Обеспечение сохранности фонда является одной из главных функций библиотек, без должного исполнения которой они с течением времени не только не смогут в должной мере удовлетворять информационные потребности пользователей, но и столкнутся с угрозой частичной либо полной потери читателей.
Обеспечить сохранность библиотечных фондов и хранящейся в них информации как части культурного наследия и обобщённого информационного ресурса России можно только при развитии таких направлений деятельности:
1. Поддержание надлежащего нормативного физического и санитарно-гигиенического состояния зданий, помещений книгохранилищ, инженерных коммуникаций.
2. Расширение площадей хранилищ соответственно увеличению библиотечных фондов, строительство и реконструкция зданий библиотек.
3. Оборудование библиотек современными техническими системами средств безопасности, их непрерывное совершенствование и обеспечение бесперебойного функционирования.
4. Непрерывное совершенствование материально-технической базы библиотек в целях обеспечения нормативного режима хранения документной информации, своевременная реставрация документов фонда.
5. Обеспечение функционирования процессов защиты, хранения и использования библиотечных фондов достаточным число квалифицированного персонала.
6. Создание единого страхового фонда документов библиотек [28, с. 230].
6
На законодательном уровне нормативно-методическое обеспечение защиты информации в библиотеках реализуется посредством разработки и утверждения документов РБА, федеральными органами исполнительной власти.
Главные угрозы для защиты информации библиотечных фондов представляют:
– характеристики материальной основы бумажного документа;
– стихийные бедствия и аварии;
– условия и режим хранения бумажных документов;
– обращение документов и их использование [9, с. 36].
Бóльшую часть фондов в библиотеках традиционно составляют документы на бумажных носителях, к которым относятся книги, газеты, журналы, альбомы, рукописи, карты, ноты и иные виды печатных изданий. Материал, из которых они изготовлены, как правило, органического происхождения. Это бумага, картон, кожа, дерево и проч. Эти материалы, к сожалению, подвержены естественному старению.
Однако, и при хранении современных носителей информации – микрофильмы, оптические и магнитные диски, цифровые носители и т. п. появляются проблемы, поскольку данные носители нуждаются в особом режиме хранения и воспроизведения во избежание преждевременного износа и частичной либо полной потери данных.

2.2. ИССЛЕДОВАТЬ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В БИБЛИОТЕКАХ

Способы, применяемые для защиты информации в библиотеках, делятся на три группы:
1) организационные способы (регулируемые внутренними документами библиотеки);
2) технологические способы (защита на основе программно-аппаратных средств);
3) правовые способы (контроль за реализацией законодательства).
Реально применяемые методы могут сочетать в себе элементы из разных категорий.
Правовые методы используются для защиты информационных ресурсов и должны включать, прежде всего, мероприятия по обеспечению соблюдения положений ФЗ «Об информации, информатизации и защите

информации» и других нормативно-правовых актов РФ, регламентирующих работу с персональными данными и устанавливающих ответственность за нарушения режима защиты, обработки и порядка использования этих данных.
Применение конкретных мер защиты зависит от категории расположения информации.
Для эффективной защиты информации на бумажных носителях от краж и несанкционированного выноса используют такие технологические способы, как противокражные системы.
Различают два типа противокражных систем: радиочастотные и электромагнитные.
Системы с электромагнитными датчиками оптимальны для применения в библиотеках. В них высокий уровень защиты печатных документов достигается благодаря небольшим размерам

электромагнитных датчиков. Так, самый популярный датчик «невидимка» – это металлическая нить на клейкой основе, размер которой 10х50 мм. Также важным критерием выбора данной противокражной системы выступает цена электромагнитных датчиков, которая достаточно низка в сопоставлении с датчиками иных типов [28, с. 231].
Системы с радиочастотными датчиками (RFID) принадлежат к оборудованию экономичного класса, однако из-за некоторых ограничений, обусловленных их принципом действия, отличаются узкой сферой использования в библиотеках.
В технологии RFID датчики не имеют возможности реактивации. Поэтому основным пробелом таких противокражных систем выступает потенциальная вероятность экранирования защитных датчиков, что может привести к их нейтрализации и препятствует защите бумажных носителей информации от краж и несанкционированного выноса.
Несмотря на это, технология RFID активно совершенствуется и становится всё более популярной для применения в целях контроля движения документов и предотвращения краж в библиотеках.
Технология радиочастотной идентификации документов в библиотеках способствует решению сразу 3-х задач:
1) идентификация и поиск документа;
2) сохранность книг и предотвращение краж;
3) идентификация пользователей [7, с. 211].

ГЛАВА III. АНТИВИРУСНЫЕ ПРОГРАММЫ, КАК СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

3.1. ОСНОВНЫЕ ГРУППЫ АНТИВИРУСНЫХ ПРОГРАММ

Для защиты электронной информации в библиотеках применяется система защиты информации, представляющая собой совокупность исполнителей, применяемых ими способов защиты информации, а также объектов защиты, организованная и функционирующая по правилам и нормам, установленным надлежащими документами в сфере защиты информации [6].
Под способом защиты информации понимают порядок и правила применения определённых принципов и средств защиты информации [6].
Техника защиты информации включает средства защиты информации, включая средства физической защиты, криптографические средства защиты, средства контроля эффективности защиты, средства и системы управления, предназначенные для обеспечения защиты информации.
Важным аспектом защиты АБИС и ЭИР, особенно защиты от нарушения целостности информации, является нейтрализация компьютерных вирусов.
Компьютерным вирусом принято называть специально написанную, обычно небольшую по размерам программу, способную самопроизвольно присоединяться к другим программам (т.е. заражать их), создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера и в другие объединенные с ним компьютеры с

целью нарушения нормальной работы программ, порчи файлов и каталогов, создания различных помех при работе на компьютере.
В зависимости от среды обитания вирусы классифицируются на загрузочные, файловые, системные, сетевые, файлово-загрузочные.
Загрузочные вирусы внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска. Файловые вирусы внедряются в основном в исполняемые файлы с расширением .com и .exe. Системные вирусы проникают в системные модули и драйверы периферийных устройств, таблицы размещения файлов и таблицы разделов. Сетевые вирусы обитают в компьютерных сетях; файлово-

загрузочные (многофункциональные) поражают загрузочные секторы дисков и файлы прикладных программ.
По способу заражения среды обитания вирусы подразделяются на резидентные, нерезидентные. Резидентные вирусы при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к другим объектам заражения, внедряется в них и выполняет свои разрушительные действия вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают оперативную память ПК и являются активными ограниченное время. Алгоритмическая особенность построения вирусов оказывает влияние на их проявление и функционирование.
Так, репликаторные программы, благодаря своему быстрому воспроизводству, приводят к переполнению основной памяти, при этом уничтожение программ-репликаторов усложняется, если воспроизводимые программы не являются точными копиями оригинала. В компьютерных сетях распространены программы-черви. Они вычисляют адреса сетевых компьютеров и рассылают по этим адресам свои копии, поддерживая между собой связь.
«Троянский конь» – это программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о чем пользователь и не догадывается (например, собирает информацию об именах и паролях, записывая их в специальный файл, доступный лишь создателю данного вируса), либо разрушает файловую систему. Логическая бомба – это программа, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логический механизм.

3.2. СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ХАРАКТЕРИСТИКИ СПОСОБОВ ЗАЩИТЫ ИНФОРМАЦИИ

В пятерку лучших программ для обеспечения компьютерной безопасности входят ESET NOD32, Kaspersky Internet Security, Dr.Web, avast! и Avira Premium Security Suite.
Последняя версия антивируса ESET NOD32 может еще до появления вируса обнаружить его, благодаря использованию функции проактивной защиты. Система NOD32 отличается низким потреблением системных ресурсов, имеет понятный и удобный интерфейс пользователя. В поиске зараженных файлов антивирус сканирует в расширенном режиме как обычные, так и упакованные в архивы файлы. Есть возможность установить требования и настройки поиска. При повреждении системы, как полном, так и частичном, NOD32 поможет восстановить систему до ее рабочего состояния. NOD32 выбирают как простые пользователи, так и многие независимые эксперты.

Программный пакет от компании «Лаборатория Касперского» - Kaspersky Internet Security хорошее решение для комплексной защиты системы. В последней версии Kaspersky было сделано много доработок, добавлено новые функции и возможности. Антивирус Касперского предоставляет надежную защиту персональных данных, содержит модуль для распознавания спама (анти-спам). Kaspersky быстро реагирует при обнаружении вирусной угрозы благодаря системе сбора информации о подозрительных программах и заражениях.
Мощная система защиты от вирусов Dr.Web использует эвристический анализатор для обнаружения вредоносных программ (вирусы, рекламное ПО, различные модификации вирусов и шпионские программы). Загрузка новых вирусных баз происходит регулярно в автоматическом режиме (несколько раз в день в базы Dr.Web добавляются данные проанализированного вирусного образца). В состав антивируса Dr.Web входит приложение SpIDer Guard - это файловый монитор, который обеспечивает перехват обращений к файлам и защиту в онлайн-режиме.
Антивирус avast! находит зараженные файлы на жестком диске, в загрузочных секторах, оперативной памяти компьютера и в электронных письмах. В составе avast! есть модуль блокировки скриптов. Русский интерфейс программы avast! отличается простотой и удобством настройки и использования, есть поддержка скинов.
Avira Premium Security Suite - антивирусное программное обеспечение с русскоязычным интерфейсом от германских разработчиков. В последней версии антивируса Avira была добавлена функция сканирования заблокированных файлов, доработан фаервол (межсетевой экран) и планировщик, самозащита антивируса. Также последняя версия программы Avira отличается улучшенной функцией лечения зараженных файлов.
В процессе проверки на вирусы рекомендуется придерживаться определённых правил:
1. Проверять на присутствие вирусов все съёмные носители информации (дискеты, CD, DVD, флэш-диски и т. д.) перед их использованием.

2. Регулярно (раз в неделю или чаще) проводить полную проверку компьютера. Для этого следует задать конкретное время автоматического начала проверок в настройках антивирусной программы.
3. Запускать антивирусный сканер в режиме полной проверки компьютера, не дожидаясь очередной автоматической проверки, если появились признаки, предположительно свидетельствующие о возможном заражении компьютера. К таким признакам относятся разного рода «странные» явления, происходящие с компьютером, например:
– вывод на экран непредусмотренных сообщений или изображений;
– подача непредусмотренных звуковых сигналов;
– неожиданное открытие и закрытие лотка CD-ROM-устройства;
– произвольный, без участия пользователя, запуск на компьютере каких-либо программ [18, с. 90].

ЗАКЛЮЧЕНИЕ

10

Информационная безопасность представляет собой такое состояние информационных ресурсов и систем, при котором обеспечивается защита данных от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т. п.
Угрозы информационной безопасности библиотечных ресурсов и информации, хранящейся в библиотеках, включают: стихийные бедствия; пожары; производственные аварии; террористические акты; кражи; перехват информации; компьютерные преступления; использование некачественных материалов для создания информационных ресурсов.
Защита информации представляет собой деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
Способ защиты информации представляет собой порядок и правила применения определённых принципов и средств защиты информации защиты информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 05.12.2016 № 646) [Электронный ресурс] // СПС КонсультантПлюс. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5434/ (дата обращения: 10.01.2019).
2. Федеральный закон от 29.12.1994 (ред. от 03.07.2016) № 78–ФЗ «О библиотечном деле» [Электронный ресурс] // СПС КонсультантПлюс. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 10.01.2019).
3. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.12.2018) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // СПС КонсультантПлюс. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 10.01.2019).
4. Постановление Правительства РФ от 21.04.2010 № 266 (ред. от 03.11.2014) «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну…» [Электронный ресурс] // СПС КонсультантПлюс. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_99819/ (дата обращения : 15.01.2019).
5. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] // СПС КонсультантПлюс. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_147084/ (дата обращения: 10.01.2019).
6. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст) [Электронный ресурс] // СПС КонсультантПлюс. – Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=STR;n=15851#02893683941665679 (дата обращения : 15.01.2019).

11

7. Абрамов, С. Б. Проблемы внедрения технологии радиочастотной идентификации в библиотеках [Текст] / С. Б. Абрамов [и др.] // Материалы междунар. конф. КРЫМ–2010. – Москва : ГПНБ России, 2010. – С. 211–217.
8. Алешин, Л. И. Безопасность в библиотеке [Текст] : учеб.-метод. пособие / Л. И. Алешин. – Москва : Либерея, 2005. – 197 с.
9. Арутюнян, А. Р. Защита информации [Текст] / А. Р. Арутюнян // Вестник научных конференций. – 2017. – №

3–5 (19). – С. 35–37.
10. Баранова, Е. Защита персональных данных: проблемы и решения [Текст] / Е. Баранова // Библиотека. – 2011. – № 1. – С. 32–35.
11. Баранова, Е. К. Информационная безопасность и защита информации [Текст] / Е. К. Баранова. – Москва : РИОР, 2018. – 256 с.
12. Бойкова, О. Защита персональных данных [Текст] / О. Бойкова // Независимый библиотечный адвокат. – 2012. – № 1. – С. 34–46.
13. Бойченко, И. С. Правовое обеспечение электронного взаимодействия при формировании информационного общества в Российской Федерации [Текст] / И. С. Бойченко // Государственная власть и местное самоуправление. – 2017.– № 1. – С. 33–37.
14. Борисов, М. А. Основы организационно-правовой защиты информации [Текст] / М. А. Борисов. – Москва : Editorial URSS, 2018. – 312 с.
15. Внуков, А. А. Защита информации [Текст] / А. А. Внуков. – Москва : Юрайт, 2017. – 242 с.
16. Герасименко, В. А. Основы защиты информации [Текст] / В. А. Герасименко, А. А. Малюк. – Москва : Инко-бук, 2017. – 537 с.
17. Гончаров, М. В. Практическая реализация библиотечного Интернет-комплекса : научно-практ. пособие [Текст] / М. В. Гончаров, К. А. Колосов. – Москва : ФАИР-ПРЕСС, 2005. – 192 с.
18. Девянин, П. Н. Модели безопасности компьютерных систем [Текст] / П. Н. Девянин. – Москва : Академия, 2015. – 144 с.
19. Джиго, А. Взаимовлияние информационно-библиотечной среды и общественных наук [Текст] / А. Джиго. – Москва : ИНИОН РАН, 2018. – 250 с.
20. Домбровская, Л. А. Современные подходы к защите информации, методы, средства и инструменты защиты [Текст] / Л. А. Домбровская, Н. А. Яковлева // Наука, техника и образование. – 2016. – № 4 (22). – С. 16–19.
21. Информационная безопасность [Текст] / под ред. В. П. Мельникова. – Москва : КноРус, 2018. – 376 с.
22. Информационные технологии : учеб. пособие [Текст] / авт.-сост. О. П. Кутькина. – Барнаул : Изд-во АлтГАКИ, 2010. – 351 с.
23. Капустин, Ф. А. Информационная безопасность и защита информации в современном обществе [Текст] / Ф. А. Капустин // Актуальные проблемы авиации и космонавтики. – 2016. – Т. 2. № 12. – С. 738–740.
12
24. Кияев, В. Безопасность информационных систем [Текст] / В. Кияев, О. Граничин. – Москва : Открытый Университет «ИНТУИТ», 2016. – 192 с.
25. Койнов, Р. С. Модель управления доступом типовой библиотечной информационной системы [Текст] / Р. С. Койнов, А. С. Добрынин // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2016. – № 4. – С. 46–54.
26. Кругликовский, А. П. Информационная безопасность электронных библиотек [Текст] / А. П. Круликовский // Проблемы информационной безопасности : сб. тр. – Симферополь, 2016. – С. 89–90.
27. Минбалеев, А. В. К вопросу об ограничении доступа к информации в библиотеках [Текст] / А. В. Минбалеев // Вестник Южно-Уральского государственного университета. Серия: Право. – 2015. – Т. 15. № 4. – С. 99–103.
28. Новоселов, П. В. Современная библиотека: идентификация и защита книг [Текст] / П. В. Новоселов // Материалы международной конференции КРЫМ-2004. – Москва : ГПНБ России, 2004. – С. 227–232.
29. Парамонов, Р. В. Информационная безопасность как территория ответственности библиотек: социальный аспект [Текст] / Р. В. Парамонов // Вестник Московского государственного университета культуры и искусств. – 2014. – № 1 (57). – С. 178–182.
30. Петраков, А. В. Основы практической защиты информации [Текст] / А. В. Петраков. – Москва : РадиоСофт, 2015. – 504 с.
31. Пилко, И. С. Информационные и библиотечные технологии : учеб. пособие [Текст] / И. С. Пилко. – СПб. : Профессия, 2006. – 342 с.
32. Пономарева, Ю. В. Вопрос соотношения права на информацию и интересов национальной безопасности в свете международного опыта [Текст] / Ю. В. Пономарева, З. В. Макарова // Вестник Южно-Уральского государственного университета. Серия: Право. – 2015. – Т. 15. № 1. – С. 91–95.
33. Стрелкова, Е. В. Сетевой объект хранения и многократного использования в эволюции управления доступом [Текст] / Е. В. Стрелкова // Доступность электронных ресурсов библиотек, музеев, архивов как актуальная проблема развития информационного общества : материалы науч.практ. конф. / ред.-сост. И. Е.

Прозоров. – Санкт-Петербург : Политехника, 2011. – С. 18−35.
34. Федякова, Н. Н. Обеспечение информационной безопасности электронной библиотеки [Текст] / Н. Н. Федякова, Э. М. Ивойлов, Р. А. Табачников // Контентус. – 2016. – № 6 (47). – С. 283–291.
35. Хачатурова, С. С. Хранение и защита информации [Текст] / С. С. Хачатурова // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 2–1. – С. 63–65.
36. Шабаршина, О. В. О роли библиотеки в формировании культуры информационной безопасности личности в современном обществе [Текст] / О. В. Шабаршина // Философия образования. – 2006. – № 1 (15). – С. 143–146.
37. Щеглов, А. Ю. Защита информации: основы теории [Текст] / А. Ю. Щеглов, К. А. Щеглов. – Москва : Юрайт, 2017. – 309 с.