МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра информационной безопасности

ПРАКТИЧЕСКАЯ РАБОТА №4

по дисциплине «Основы информационной безопасности»

Тема: «Определение уровня защищённости ИСПДн и реализация требований к ИС в соответствии в руководящим документом ФСТЭК»

Студентка гр. 0361 _____ Солонухина А.Л.

Преподаватель _____ Воробьёв Е.Г.

Санкт-Петербург
2022

Постановка задачи

Цель работы: изучение вида работ по определению необходимого уровня защищенности персональных данных в конкретной организации.

1. Описываемая область выбирается на основе собранных материалов по конкретному предприятию, организации или компании.
2. Отчет выполняется с проведением анализа уровня защищенности информационных системах персональных данных и реализации требований к ИС в соответствии с руководящим документом ФСТЭК: «Методика оценки угроз безопасности информации» утверждённый ФСТЭК России 5 февраля 2021 г.

УТВЕРЖДАЮ

Ректор НГУ

Владимиров В.В.

«30» ноября 2022 г.

Модель угроз безопасности информации

«Электронная библиотечная система НГУ (Некого Государственного Университета)»

1. Общие положения

Модель угроз безопасности информации разработана для организации «НГУ (Некий Государственный Университет)».

Модель угроз разрабатона в соответствии со следующими нормативными и методологическими документами:

ФЗ № 149 «Об информации, информационных технологиях и о защите информации»;

ФЗ № 152 «О персональных данных»;

Методический документ «Методика оценки угроз безопасности информации» утверждённый ФСТЭК России 5 февраля 2021 г.

Обладатель информации, заказчик и оператор систем и сетей – НГУ.

За обеспечение защиты информации (безопасности) систем и сетей несёт ответственность подразделение «Отдел информационной безопасности НГУ».

2. Описание систем и сетей и их характеристика как объектов защиты

Модель угроз безопасности информации разработана для ЭБС (электронной библиотечной системы) и локальной сети библиотеки, расположенных в пределах НГУ.

Класс защищённости ЭБС – 1Д (многопользовательская система с разными уровнями доступа и разными уровнями конфиденциальности информации, в которой циркулируют персональные данные). Классификация приведена в соответствии с Руководящим Документом Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

В ЭБС обрабатываются общедоступные персональные данные пользователей: сотрудников и не являющихся сотрудниками организации, актуальны угрозы 1 типа (наличие недекларированных возможностей в системном ПО) – уровень защищённости ИСПДн - 2УЗ.

Нормативные правовые акты РФ, в соответствии с которыми функционируют указанные система и сеть: ФЗ №152 «О персональных данных», ФЗ №273 «Об образовании в Российской Федерации», Указ Президента РФ №188 «Об утверждении Перечня сведений конфиденциального характера», ФЗ №78 «О библиотечном деле», ФЗ №5351-1 «Об авторском праве и смежных правах».

Назначение ЭБС и локальной сети библиотеки НГУ: содействие вузу в выполнении учебно-воспитательного процесса и научно-исследовательских работ; развитие и совершенствование справочно-библиографического аппарата библиотеки; обеспечение доступности информации.

Основные задачи (функции) ЭБС и локальной сети библиотеки НГУ:

1) обеспечение круглосуточного онлайн-доступа к чтению электронных книг, хранящихся на общем сервере;

2) возможность приобретения платного абонемента с дополнительными привилегиями;

3) добавление и хранение книг на общем сервере;

4) автоматизированный поиск и обработка ресурсов электронной библиотеки;

5) возможность удалённого доступа к ЭБС через Личный кабинет на сайте библиотеки НГУ;

6) возможность доступа к ЭБС через персональные компьютеры из библиотеки, расположенной в здании НГУ;

7) защита данных пользователей и обеспечение информационной безопасности ресурсов.

Состав обрабатываемой информации:

1) учётные данные пользователей ЭБС и сотрудников НГУ, взаимодействующих с системой: фамилия, имя, отчество, дата рождения, адрес эл. почты, номер мобильного телефона, должность/информация об обучении в вузе, данные о публикации электронных книг, история просмотра электронных книг, данные о совершённых платежах.

2) информация, касающаяся платежей, проводящихся для оформления подписки;

3) информационные ресурсы библиотеки (электронные материалы).

Для доступа в систему требуется авторизация пользователей. В системе присутствует деление пользователей по типам доступа на группы:

1) обычные – с бесплатной подпиской, предоставляется доступ к ограниченному объему ресурсов электронной библиотеки;

2) с платной подпиской – доступ к полному объему ресурсов электронной библиотеки;

3) авторы – сотрудники НГУ, имеющие право размещать материалы в электронной библиотеке;

4) администратор ЭБС – создают группы пользователей, управляют их доступом к системе и имеют возможность смотреть пользовательскую и групповую статистику;

5) Каталогизатор ЭБС – выполняет операции каталогизации и систематизации изданий, т.е. функции по формированию баз данных каталогов ЭБС.

Доступ к ресурсам ЭБС обеспечивается удалённо, через сайт библиотеки НГУ, или с персональных компьютеров, расположенных в локальной сети читального зала НГУ.

В состав ЭБС входят компоненты: 1 АРМ администратора системы, 1 АРМ каталогизатора, 20 АРМ пользователей, веб-сайт, СУБД (PostgreSQL), 3 сервера: сервер БД (Windows Server), веб-сервер (Windows Server) и файловый сервер (Windows Server).

АРМ в локальной сети связаны линейно с использованием оптоволоконных линий связи, взаимодействуют при помощи коммутаторов, в серверной находится маршрутизатор. При обмене данными с внешней средой используется межсетевой экран (файрволл). Схема расположения и связи компонентов показана на рисунке 1.

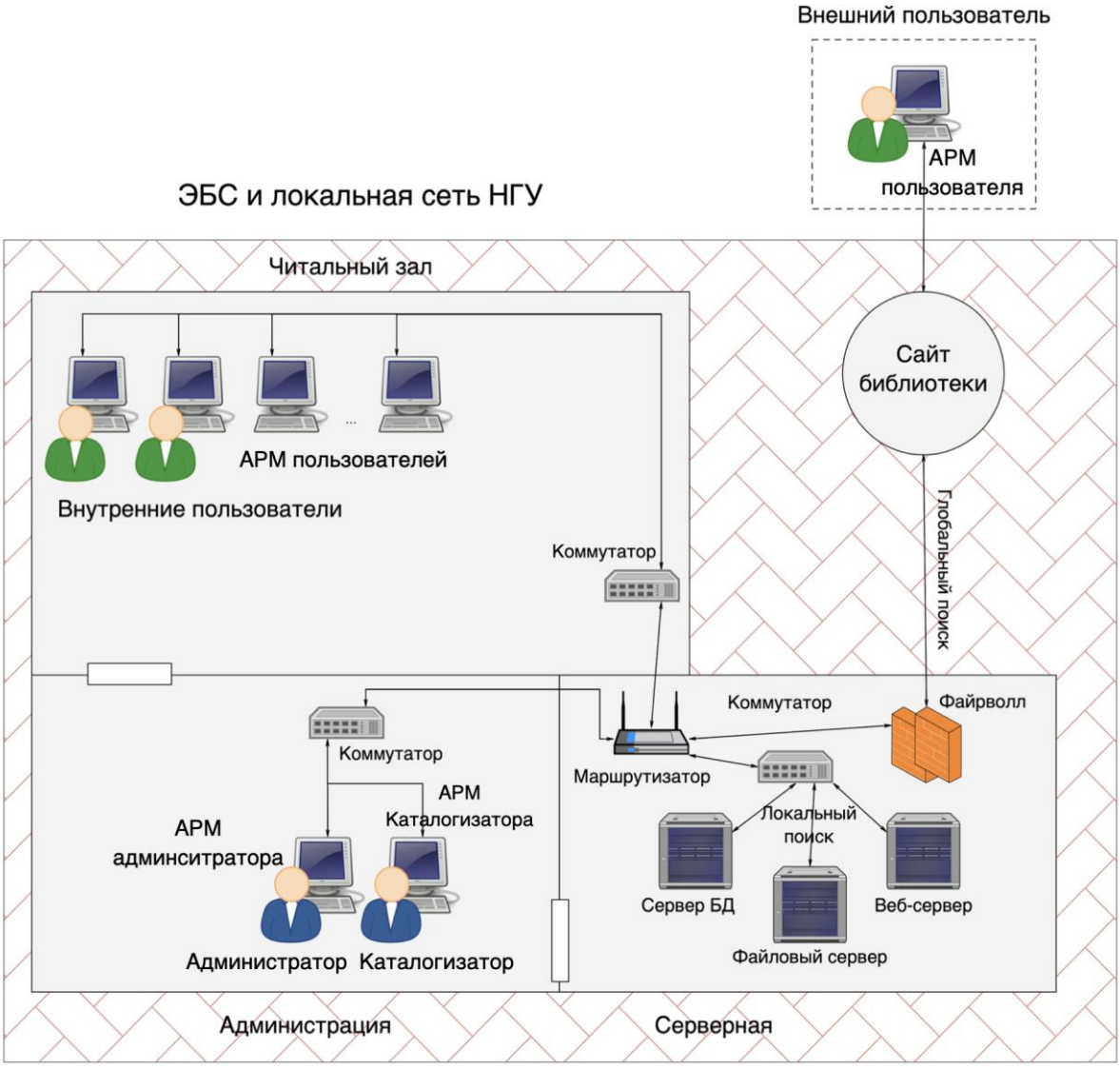

Рисунок 1 – Схема расположения и связи компонентов ЭБС и локальной сети библиотеки НГУ

ЭБС НГУ является оператором услуг: приложения, связующее ПО, ОС, аппаратная платформа, сетевая инфраструктура и система хранения данных. Вместе с тем является поставщиком услуг: данные. Поэтому ЭБС НГУ является преимущественно оператором услуг.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

Основным ресурсом ЭБС является информация в цифровом виде, хранящаяся в базах данных и передаваемая по каналам связи между пользователями и ЭБС, в том числе персональные данные, подлежащие защите в соответствии с ФЗ «О персональных данных», и информация, защищаемая законом «Об авторском праве и смежных правах».

Негативные последствия от реализации угроз безопасности информации связаны с нарушением конфиденциальности этой информации, в результате которого нарушаются права субъектов персональных данных и соответствующие законы. Негативные последствия, актуальные для ЭБС НГУ, приведены в таблице 1.

Таблица 1 – Негативные последствия от реализации угроз безопасности информации, актуальные для ЭБС НГУ

№	Виды риска (ущерба)	Возможные негативные последствия
У1	Ущерб физическому лицу	Нарушение конфиденциальности (утечка) персональных данных
		Нарушение иных прав и свобод гражданина, закрепленных в Конституции РФ и федеральных законах
У2	Риски юридическому лицу, связанные с хозяйственной деятельностью	Нарушение законодательства РФ

		Необходимость дополнительных затрат на выплаты штрафов
		Потеря (хищение) денежных средств
		Нарушение штатного режима функционирования автоматизированной системы
		Невозможность решения задач или снижение эффективности решения задач
		Публикация недостоверной информации на веб-ресурсах организации

4. Возможные объекты воздействия угроз безопасности информации

Компоненты, указанные на схеме ЭБС и локальной сети библиотеки НГУ (рисунок 1) участвуют в обработке и хранении защищаемой информации и обеспечивают реализацию основных процессов в ЭБС:

Основные информационные ресурсы и компоненты системы:

1) База аутентификационных данных;
2) СУБД;
3) файловый сервер;
4) веб-сервер;
5) веб-сайт ЭБС;
6) сервер БД;
7) ПО для администрирования,
8) АРМ (автоматизированные рабочие места), расположенные в библиотеке НГУ,
9) проводные и беспроводные каналы передачи данных.

Виды воздействия для определенных выше информационных ресурсов и компонентов системы, которые могут привести к негативным последствиям, представлены в таблице 2.

Таблица 2 – Объекты воздействия и виды негативного воздействия на них

Негативные последствия	Объекты воздействия	Виды воздействия
Нарушение конфиденциальности (утечка) персональных данных физических лиц (У1)	База аутентификационных данных	Утечка аутентификационных данных пользователей из БД
	АРМ, расположенные в библиотеке НГУ	Утечка учетной информации, вводимой пользователями при использовании АРМ
	Проводные и беспроводные каналы передачи данных	Перехват информации, содержащей учетные данные пользователей, передаваемой по каналам
Нарушение иных прав и свобод гражданина, закрепленных в Конституции РФ и федеральных законах (У1)	Файловый сервер	Утечка материалов ЭБС, защищаемых авторским правом
	АРМ, расположенные в библиотеке НГУ	Утечка материалов ЭБС, защищаемых авторским правом
Нарушение законодательства РФ, необходимость дополнительных затрат на выплаты штрафов (У2)	База аутентификационных данных	Утечка аутентификационных данных пользователей, защищаемых законом «О персональных данных» (предусмотрены штрафы)
	Файловый сервер	Утечка материалов ЭБС, защищаемых законом «Об авторском праве и смежных

		правах» (предусмотрены штрафы)
Потеря (хищение) денежных средств (У2)	Веб-сайт ЭБС	Подмена данных при совершении пользователем платежа (покупка платной подписка)
Нарушение штатного режима функционирования автоматизированной системы, невозможность решения задач или снижение эффективности решения задач (У2)	ПО для администрирования	Несанкционированный доступ, нарушение функционирования программно- аппаратных средств администрирования ЭБС
	АРМ, расположенные в библиотеке НГУ	Нарушение функционирования АРМ
	Файловый сервер	Нарушение функционирования ЭБС (удаление информации, необходимой для решения задач ЭБС)
Публикация недостоверной информации на веб-ресурсах организации (У2)	Файловый сервер	Несанкционированная модификация, подмена, искажение информации
	СУБД	Несанкционированная модификация, подмена, искажение информации

Схема описанных выше объектов воздействия и содержащейся в них защищаемой информации приведена на рисунке 2.

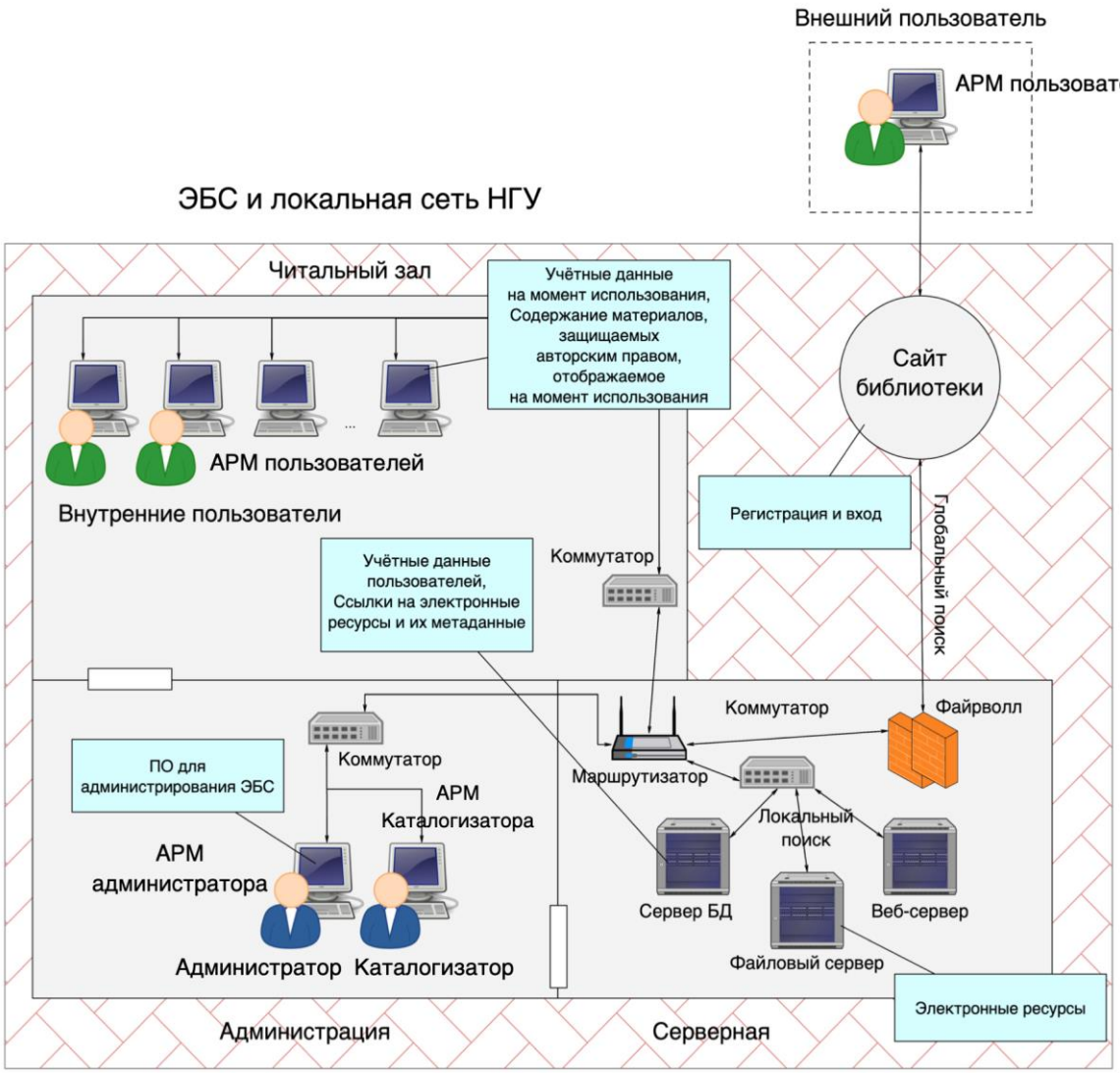

Рисунок 2 – Схема объектов воздействия и содержащейся в них защищаемой информации

5. Источники угроз безопасности информации

Актуальными нарушителями (антропогенными источниками угроз) безопасности информации для ЭБС и локальной сети библиотеки НГУ являются:

1) хакеры;
2) конкурирующие организации;
3) администраторы ЭБС;
4) авторизованные пользователи ЭБС;

Для перечисленных нарушителей определены категории (по признаку принадлежности к системе) и возможные цели реализации ими угроз безопасности информации, которые приведены в таблице 3.

Таблица 3 – Возможные цели реализации угроз безопасности информации для нарушителей в ЭБС НГУ

№	Виды актуального нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Хакеры	Внешний	Получение финансовой или иной материальной выгоды
2	Конкурирующие организации	Внешний	Получение материальной выгоды
3	Администраторы ЭБС	Внутренний	Получение финансовой или иной материальной выгоды
			Непреднамеренные, неосторожные или неквалифицированные действия
4	Авторизованные пользователи ЭБС	Внутренний	Получение финансовой или материальной выгоды
			Любопытство или желание самореализации
			Месть за ранее совершенные действия
			Непреднамеренные, неосторожные или неквалифицированные действия

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны ЭБС.

Внутренние нарушители ЭБС имеют разный уровень прав доступа к информационным ресурсам и компонентам системы:

1) Авторизованные пользователи ЭБС имеют пользовательские права доступа (доступ в личный кабинет на веб-сайте, к АРМ в читальном зале библиотеки).

2) Администраторы ЭБС имеют привилегированные права доступа (доступ к соответствующим АРМ и ПО администрирования).

Результат определения актуальных нарушителей при реализации угроз безопасности информации в ЭБС НГУ представлен в таблице 4.

Таблица 4 – Результат определения актуальных нарушителей при реализации угроз безопасности информации в ЭБС НГУ

№	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1: нарушение конфиденциальности (утечка) персональных данных; нарушение иных прав и свобод гражданина, закрепленных в Конституции РФ и федеральных законах	Хакеры	Внешний	Н2 (базовые повышенные возможности)
		Конкурирующие организации	Внешний	Н2 (базовые повышенные возможности)
		Администраторы ЭБС	Внутренний	Н2 (базовые повышенные возможности)
		Авторизованные пользователи ЭБС	Внутренний	Н1 (базовые возможности)
2	У2: нарушение законодательства РФ; необходимость дополнительных затрат на выплаты штрафов;	Хакеры	Внешний	Н2 (базовые повышенные возможности)
		Конкурирующие организации	Внешний	Н2 (базовые повышенные возможности)

	потеря (хищение) денежных средств; нарушение штатного режима функционирования автоматизированной системы; невозможность решения задач или снижение эффективности решения задач; публикация недостоверной информации на веб-ресурсах организации	Администраторы ЭБС	Внутренний	H2 (базовые повышенные возможности)
		Авторизованные пользователи ЭБС	Внутренний	H1 (базовые возможности)

6. Способы реализации (возникновения) угроз безопасности информации

Предполагается, что нарушитель уровня H1 имеет:

1) доступные в свободной продаже технические средства и программное обеспечение.

Предполагается, что нарушитель уровня H2 имеет:

1) доступные в свободной продаже технические средства и программное обеспечение;

2) специально разработанные технические средства и программное обеспечение.

Актуальные для ЭБС НГУ способы реализации угроз безопасности информации и соответствующие им виды нарушителей (и их возможности) представлены в таблице 5.

Таблица 5 – Актуальные для ЭБС НГУ способы реализации угроз безопасности информации и соответствующие им виды нарушителей

№	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации

1	Хакеры, Конкурирующие организации (Н2)	Внешний	База аутентификационных данных: утечка аутентификационных данных пользователей из БД	Пользовательский веб-интерфейс сайта библиотеки НГУ	Использование уязвимостей проверки данных, нестойкой криптографии и некорректной настройки прав доступа; Инъекции
			Файловый сервер: утечка материалов ЭБС, защищаемых авторским правом; нарушение функционирования ЭБС (удаление информации, необходимой для решения задач ЭБС); несанкционированная модификация, подмена, искажение информации	Пользовательский интерфейс доступа к файловому серверу ЭБС	Использование уязвимостей ПО, предназначенного для доступа пользователей к ресурсам файлового сервера
			Веб-сайт ЭБС: подмена данных при совершении пользователем платежа (покупка платной подписка) несанкционированный доступ к пользовательским аккаунтам и ресурсам веб-сайта	Пользовательский веб-интерфейс сайта библиотеки НГУ	Использование уязвимостей кода веб-сайта Обнаружение доступных директорий веб-сайта Атаки Обход механизмов разграничения доступа Подбор аутентификационных данных пользовательского аккаунта с помощью специальных программных средств или вручную
2	Администраторы ЭБС (Н2)	Внутренний	АРМ, расположенные в библиотеке НГУ: утечка аутентификационной информации, вводимой пользователями при использовании АРМ; утечка электронных материалов ЭБС; нарушение функционирования АРМ	ПО для администрирования системы (системные и сетевые утилиты)	Ошибочные действия при настройке ПО для администрирования Внедрение вредоносного ПО через средства установки/обновления ПО
				Оперативное или постоянное запоминающее устройство АРМ	Осуществление несанкционированного доступа к оперативным или постоянным запоминающим устройствам АРМ

				Съемные носители информации	Внедрение вредоносного ПО через съемные носители информации
3	Авторизованные пользователи ЭБС (Н1)	Внутренний	АРМ, расположенные в библиотеке НГУ: утечка аутентификационной информации, вводимой пользователями при использовании АРМ; утечка материалов ЭБС, защищаемых авторским правом; нарушение функционирования АРМ; сброс состояния оперативной памяти отдельных устройств, блоков или системы в целом	АРМ, расположенные в библиотеке НГУ	Ошибочные действия при пользовании АРМ
				Съемные носители информации	Внедрение вредоносного ПО через съемные носители информации
			Проводные каналы передачи данных: Перехват информации, передаваемой по каналам	Коммутатор локальной сети	Подключение стороннего устройства к порту коммутатора и использование утилит для перехвата передаваемой в сети информации

7. Актуальные угрозы безопасности информации

При разработке описаний возможных угроз безопасности информации учитывались:

1) актуальные нарушители и уровни их возможностей;
2) объекты воздействия, находящиеся в составе ЭБС;
3) основные способы реализации угроз безопасности информации;
4) возможные негативные последствия реализации угроз.

Перечень возможных угроз безопасности информации ЭБС НГУ, описанных в соответствии с перечисленными выше факторами, приведён в таблице 6.

Таблица 6 – Возможные угрозы безопасности информации ЭБС НГУ

№	Наименование угрозы	Нарушители	Объекты воздействия	Способы реализации	Возможные последствия
1	Угроза утечки информации	Хакеры (Н2), Конкурирующие организации (Н2)	Файловый сервер	Использование уязвимостей ПО, предназначенного для доступа пользователей к ресурсам файлового сервера	Утечка материалов ЭБС, защищаемых авторским правом; нарушение функционирования ЭБС (удаление информации, необходимой для решения задач ЭБС); несанкционированная модификация, подмена, искажение информации
		Авторизованные пользователи ЭБС (Н1)	Проводные каналы передачи данных	Подключение стороннего устройства к порту коммутатора и использование утилит для перехвата передаваемой в сети информации	Перехват информации, передаваемой по каналам
2	Угроза несанкционированного доступа	Администраторы ЭБС (Н2)	АРМ, расположенные в библиотеке НГУ	Осуществление несанкционированного доступа к оперативным или постоянным запоминающим устройствам АРМ	Утечка аутентификационной информации, вводимой пользователями при использовании АРМ
		Хакеры (Н2), Конкурирующие организации (Н2)	Веб-сайт ЭБС,	Подбор аутентификационных данных пользовательского аккаунта с помощью специальных программных средств или вручную	Несанкционированный доступ к пользовательским аккаунтам и ресурсам веб-сайта
		Хакеры (Н2), Конкурирующие	Пользовательский веб-интерфейс сайта	Использование уязвимостей проверки данных и некорректной	Утечка аутентификационных данных пользователей из БД

		организации (Н2)	библиотеки НГУ	настройки прав доступа; Инъекции	
3	Угроза удаления информационных ресурсов	Авторизованные пользователи ЭБС (Н1), Администраторы ЭБС (Н2)	АРМ, расположенные в библиотеке НГУ	Внедрение вредоносного ПО через съемные носители информации	Нарушение функционирования АРМ; уничтожение электронных материалов ЭБС
		Авторизованные пользователи ЭБС (Н1)	АРМ, расположенные в библиотеке НГУ	Ошибочные действия при пользовании АРМ	Сброс состояния оперативной памяти отдельных устройств, блоков или системы в целом

Возможные сценарии реализации угроз безопасности информации для ЭБС НГУ:

1) Возможный сценарий реализации угрозы удаления информационных ресурсов состоит из четырёх последовательных тактик: Т1, Т2, Т3, Т10 и соответствующих им техник (таблица 7).

Таблица 7 – Сценарий реализации угрозы удаления информационных ресурсов

Тактика	Техники
Т1. Сбор информации о системе	Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии
Т2. Получение первоначального доступа к компонентам систем и сетей	Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций

Т3. Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
Т10. Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей

Схема реализации приведенного сценария показана на рисунке 3.

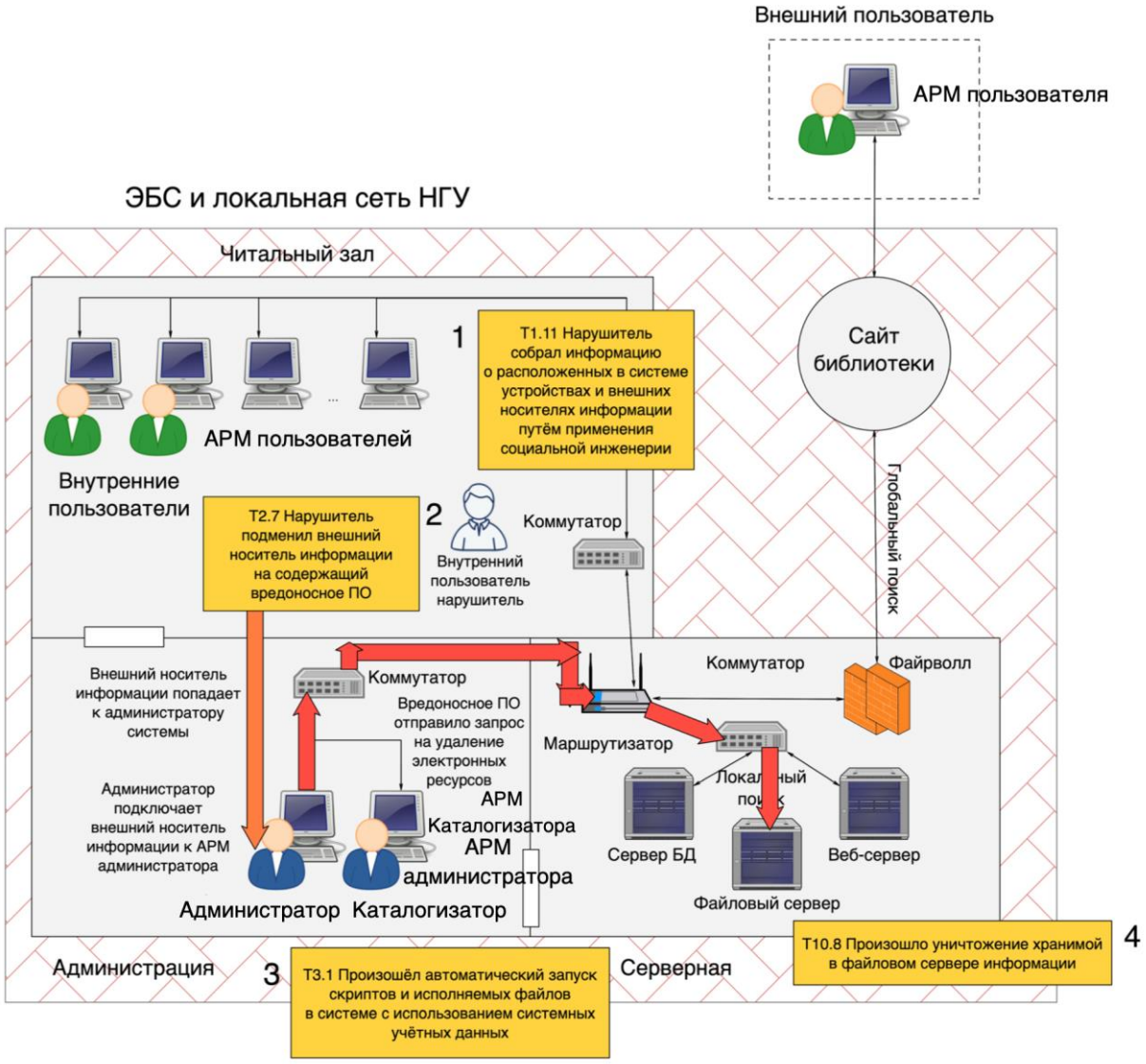

Рисунок 3 – Схема возможного сценария реализации угрозы удаления информационных ресурсов

2) Возможный сценарий реализации угрозы утечки информации состоит из четырёх последовательных тактик: Т1, Т2, Т7, Т10 и соответствующих им техник (таблица 8).

Таблица 8 – Сценарий реализации угрозы утечки информации

Тактика	Техники
Т1. Сбор информации о системе	Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии
Т2. Получение первоначального доступа к компонентам систем и сетей	Т2.9. Несанкционированное подключение внешних устройств.
Т7. Сокрытие действий и применяемых при этом средств от обнаружения	Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения: использование снифферов (сетевых анализаторов)
Т10. Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

Схема реализации приведенного сценария показана на рисунке 4.

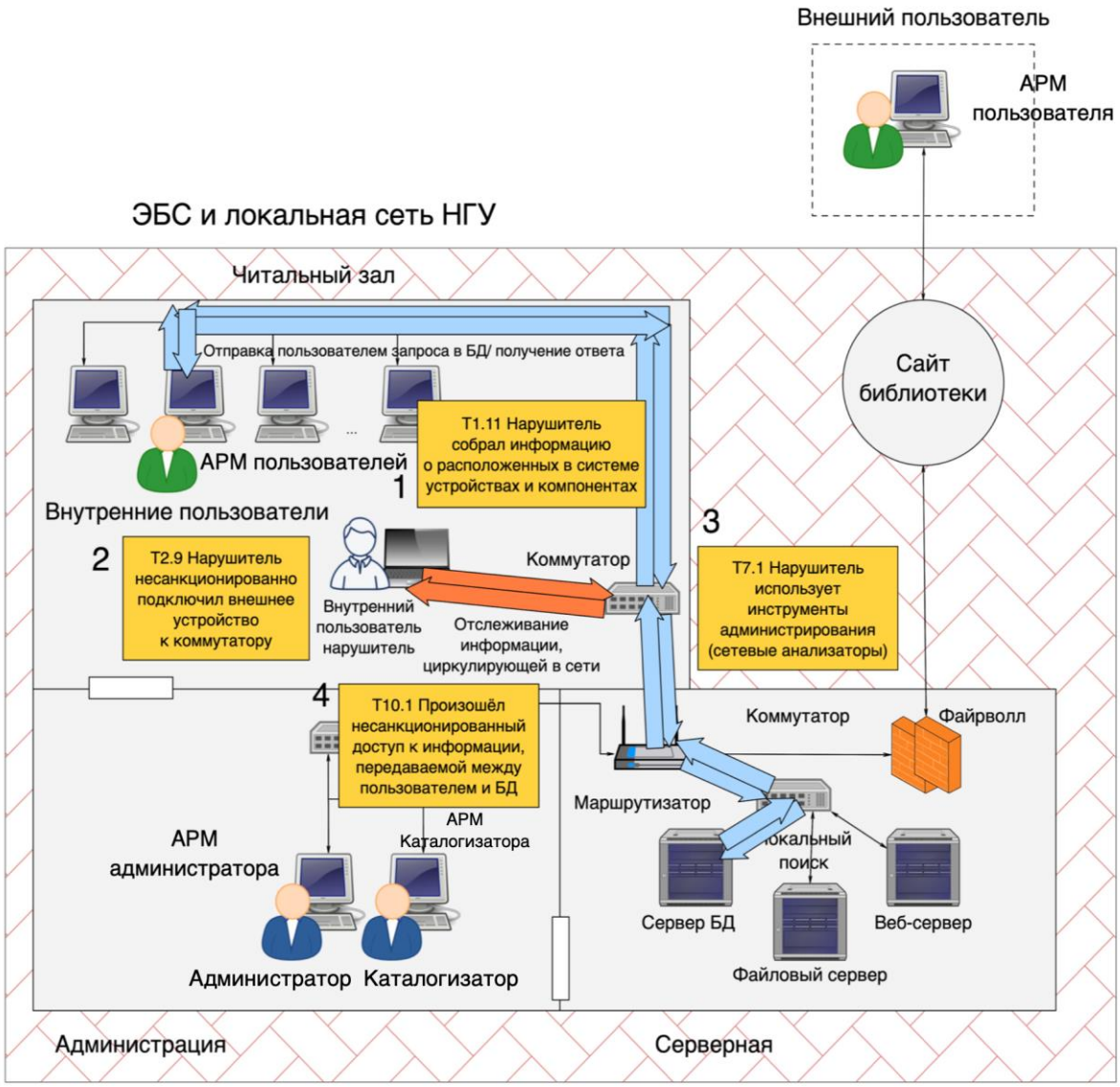

Рисунок 4 – Схема возможного сценария реализации угрозы утечки данных

3) Возможный сценарий реализации угрозы несанкционированного доступа состоит из трёх последовательных тактик: Т1, Т2, Т10 и соответствующих им техник (таблица 9).

Таблица 9 – Сценарий реализации угрозы несанкционированного доступа

Тактика	Техники

Т1. Сбор информации о системе	Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора
	Т1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
Т2. Получение первоначального доступа к компонентам систем и сетей	Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)
Т10. Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

Схема реализации приведенного сценария показана на рисунке 5.

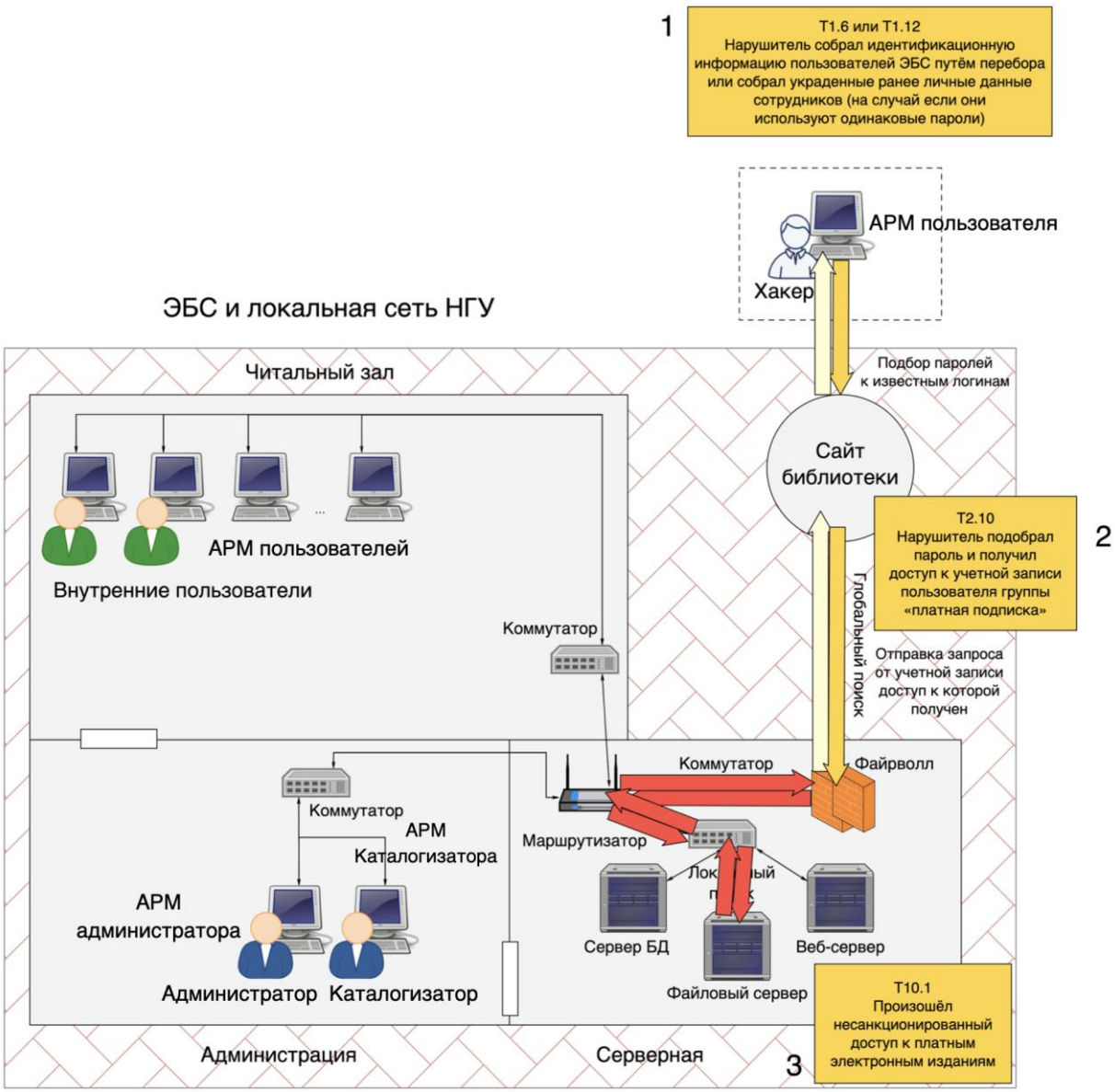

Рисунок 5 – Схема возможного сценария реализации угрозы несанкционированного доступа

Выводы

В ходе составления модели угроз безопасности информации для ЭБС и локальной сети НГУ признаны актуальными следующие угрозы:

1) Угроза несанкционированного доступа;
2) Угроза утечки информации;
3) Угроза удаления информационных ресурсов.

Для перечисленных угроз построены возможные сценарии реализации.