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

ПРАКТИЧЕСКАЯ РАБОТА №5

по дисциплине «Основы информационной безопасности»

Тема: «Спецификация объекта защиты и среды безопасности на примере курсовой работы»

Студентка гр. 0361 _____ Солонухина А.Л.

Преподаватель _____ Воробьёв Е.Г.

Санкт-Петербург

2022

Постановка задачи

1. Описываемая область выбирается студентом на основе собранных материалов по конкретному предприятию, организации или компании.
2. Цель работы: изучение вида работ по спецификации объекта защиты.
3. Отчет выполняется в форме спецификации объекта защиты и среды безопасности
4. Материал должен содержать титульный лист, постановку задачи, а также следующие разделы:
    a. Описание функций объекта
    b. Доступ на объект
    c. Персонал объекта
    d. Технические характеристики объекта
    e. Безопасность объекта
    f. Правила доступа к сетям и устройствам на предприятии
    g. Описание структуры и оценка защищенности компании (например, при помощи программного обеспечения "РискМенеджер - Анализ v3.5" или согласно методике Вихорева)
    h. Показатели исходной защищенности ИСПДн
    i. Заключение о степени защищенности

Описываемый объект – ЭБС (электронная библиотечная система) и локальная сеть библиотеки НГУ (Некого Государственного Университета).

1. Описание функций объекта

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 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.

2. Доступ на объект

ЭБС и локальная сеть библиотеки НГУ физически располагаются в здании НГУ и относятся на учебно-вспомогательной площади университета. Объект занимает 3 комнаты: читальный зал, административное помещение и серверное помещение.

Доступ в читальный зал осуществляется в рамках доступа на территорию университета – система контроля и управления доступом (СКУД) с проходной:

- турникеты (блокирующие устройства);
- пост дежурного.

Вход в автоматическом режиме, по постоянным картам студентов и сотрудников. Реализована защита от двойного прохода по одной карте.

Доступ в административное и серверное помещения ограничен электромагнитными замками – 1 на двери в администраторскую, 1 на двери в серверную (со считывателями постоянных карт сотрудников НГУ).

На территории НГУ также действуют:

- система видеоконтроля (СВК);
- система пожарной сигнализации (СПС);

Территория библиотеки НГУ разделена на зоны доступа. Деление зон по категориям приведено в таблице 1.

Таблица 1 – Категории зон доступа

Категория зоны	Наименование зоны	Функциональное назначение	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны	Наличие технических средств охраны
3	Режимная зона	Читальный зал с компьютерами	По служебным пропускам	По пропускам	Есть	Система контроля доступа, видеонаблюдение
4	Зона усиленной защиты	Администраторская, серверная	По спец. пропускам	По спец. пропускам	Есть	Охранная сигнализация, система контроля доступа, видеонаблюдение

3. Персонал объекта

Объект обслуживается:

- администраторским отделом – занимается управлением локальной сетью, разграничением прав доступа в сети, регистрацией новых пользователей и каталогизацией эл. ресурсов в ЭБС;
- отделом технического обеспечения НГУ – занимается обслуживанием и ремонтом технических средств, установленных на территории объекта.

В администраторский отдел входят: системный администратор – 1 человек, каталогизатор – 1 человек.

В отдел технического обеспечения НГУ входят: техники – 3 человека.

Электронные материалы для каталога предоставляются научными сотрудниками университета.

4. Технические характеристики объекта

Для работы с документами в читальном зале организовано 35 посадочных места, в том числе – 20 автоматизированных, с доступом в интернет, объединённых в локальную сеть.

АРМ в локальной сети связаны линейно с использованием оптоволоконных линий связи, взаимодействуют при помощи коммутаторов (в читальном зале – 1, в административном помещении – 1) и маршрутизатора (в серверном помещении – 1).

Административное помещение оснащено двумя АРМ с установленным ПО для администрирования (VMware Workspace One Access и консоль администрирования VMware Identity Manage) и СУБД (PostgreSQL) – для управления ЭБС функционирует система «ИРБИС», в её состав входит ПО, установленное на АРМ читателей, АРМ администратора и АРМ каталогизатора.

В серверном помещении расположены: 1 сервер БД, 1 файловый сервер и 1 веб-сервер. Базовое ПО, используемое для поддержки серверов - Windows Server.

5. Безопасность объекта

Данные хранятся на трёх серверах: БД аутентификационных данных, БД каталог с метаданными и ссылками на электронные материалы, каталог электронных материалов (на файловом сервере).

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).

Персональные данные, обрабатываемые в системе, относятся к категории **общедоступные**, т.е. **ИСПДн-О**.

Согласно приказу ФСТЭК №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», ЭБС НГУ имеет **класс защищенности ГИС К3** (таблица 2):

- масштаб информационной системы – объектовый (в пределах объекта библиотека НГУ);
- уровень значимости информации – УЗ 3 (в результате нарушения одного из свойств безопасности информации возможны незначительные негативные последствия в социальной, экономической и финансовой областях деятельности организации, а ИС и оператор информации могут выполнять возложенные на них функции с недостаточной эффективностью).

Таблица 2 – Классы защищенности ГИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

В соответствии с ФЗ «О безопасности критической информационной инфраструктуры РФ» так как ЭБС НГУ функционирует в сфере науки, она **относится к КИИ**, а именно: электронные образовательные и научные материалы, содержащиеся на файловом сервере и их метаданные, содержащиеся на сервере БД.

Так как ни один из показателей критериев значимости, указанных в Постановлении Правительства РФ № 127, неприменим, **категория значимости объекту не присваивается**.

На рисунке 1 представлено деление ЭБС НГУ на сегменты.

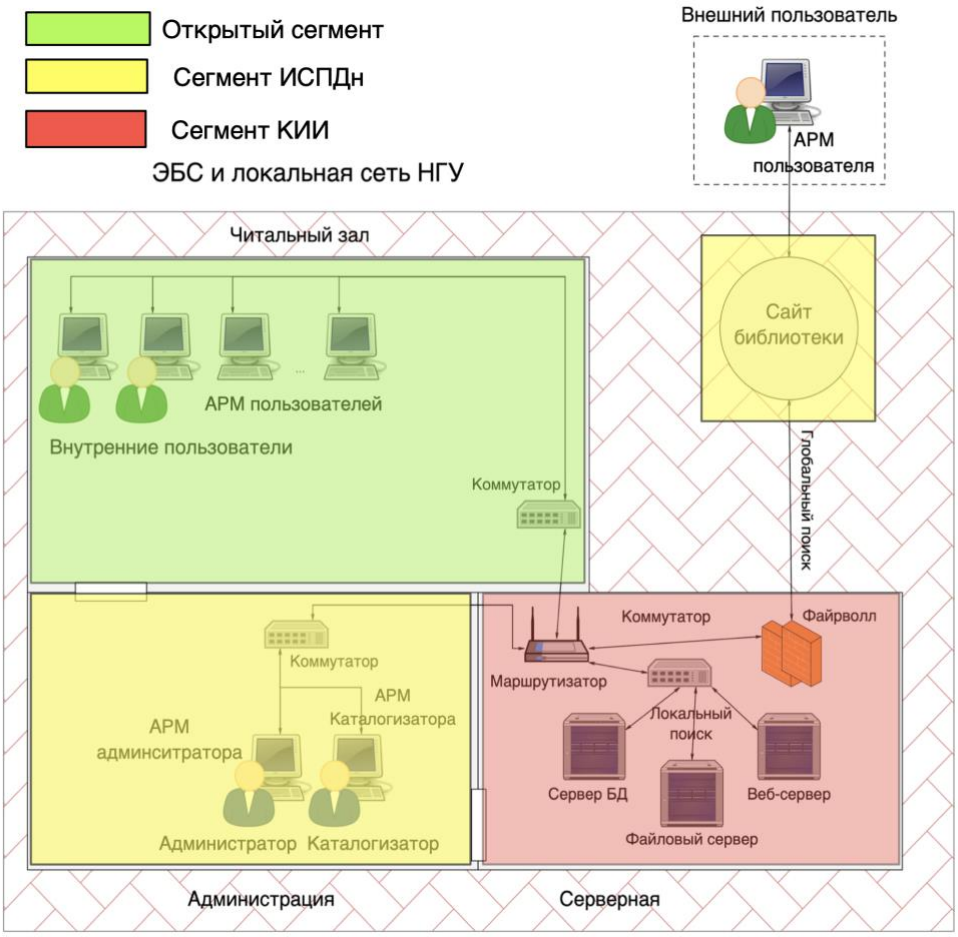

Рисунок 1 – Деление ЭБС НГУ на сегменты

Системный администратор отвечает за регулярное резервное копирование данных, и разграничение прав доступа к данным между пользователями.

Веб-сервер предназначен для хостинга сайта библиотеки НГУ. При обмене данными с внешней средой используется сетевой экран (файрволл).

Все помещения оборудованы охранно-пожарной сигнализацией и системой видеонаблюдения. За безопасность объекта в составе университета отвечают Отдел информационной безопасности НГУ и отдел комплексной безопасности НГУ.

6. Правила доступа к сетям и устройствам

Доступ к сети Интернет осуществляется только с установленных в библиотеке АРМ.

У каждого сотрудника в системе имеется свой профиль с определенным набором прав доступа к сети, защищенный паролем. Пользователи в читательском зале используют один общий профиль с известным паролем (сообщает сотрудник).

7. Описание структуры и оценка защищенности компании

Структурная схема ЭБС приведена на рисунке 2.

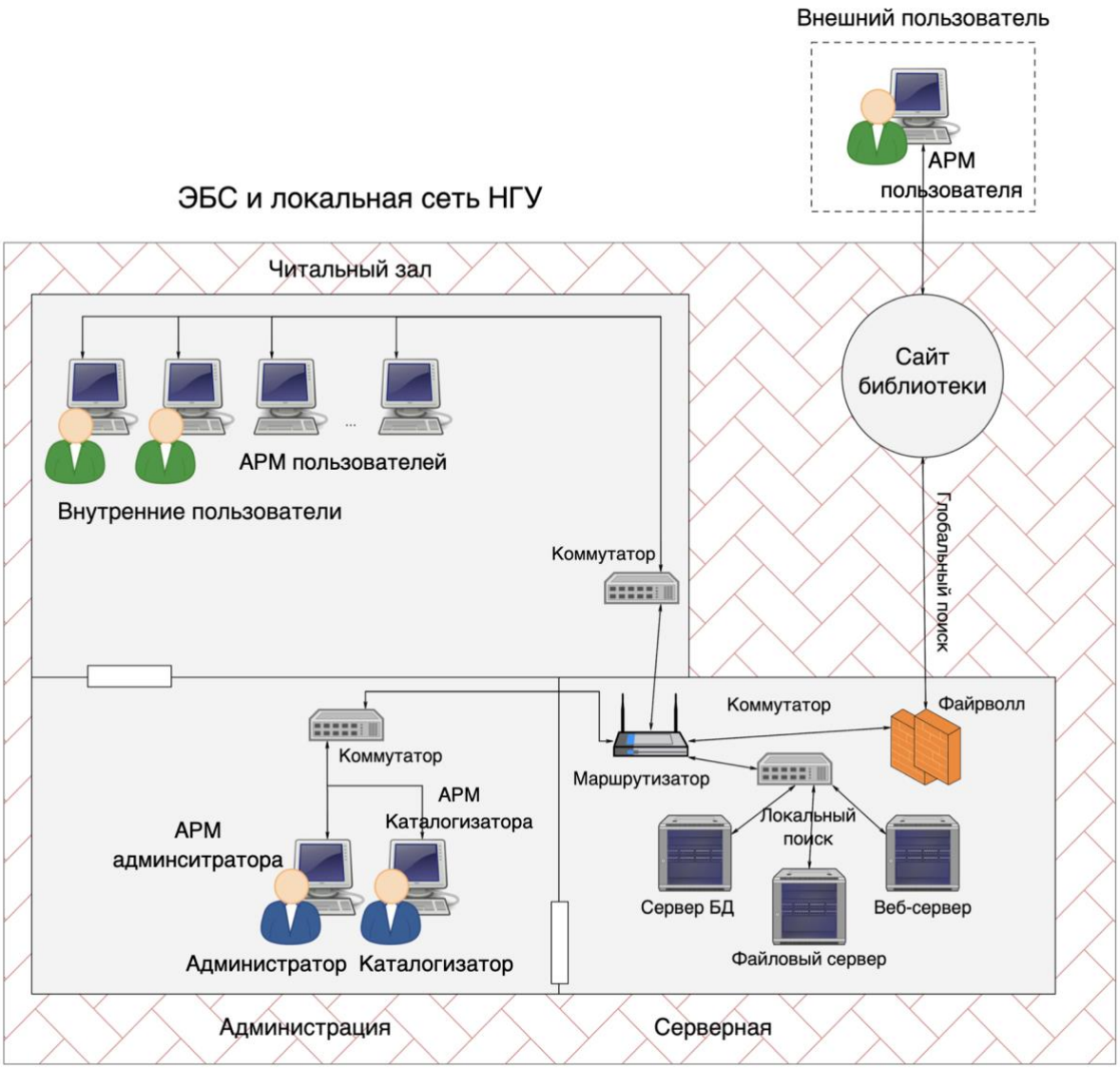

Рисунок 2 – Схема ЭБС НГУ

Структурное описание ЭБС НГУ построено в Риск Менеджер (рисунок 3).

Рисунок 3 – Структурное описание оцениваемой системы

Оценка защищенности объекта проведена по методике С.В. Вихорева (таблица 3).

Таблица 3 – Анкета для получения исходных данных по оценке приоритетности целей ИБ

	Содержание вопроса	Да	Нет
1	Может ли несанкционированное разглашение защищаемых сведений:		
1.1	⇒ привести к срыву реализации стратегических планов развития организации, повлиять на снижение ее деловой активности	да	
1.2	⇒ привести к разглашению секретов организации или третьих лиц, ноу-хау, персональных данных, нарушить тайну сообщений	да	
1.3	⇒ повлиять на ухудшение взаимоотношений с партнерами, снижение престижа и деловой репутации организации	да	
	Сумма положительных («Да») ответов по п.1, ∑(«Да») = $(К_п)_к$	3	
2	Может ли несанкционированное изменение защищаемой информации:		
2.1	⇒ привести к принятию ошибочных решений (или непринятию вообще), важных для практической деятельности организации	да	
2.3	⇒ привести к полной или частичной дезорганизации деятельности организации или ее подразделений, нарушить взаимоотношения с партнерами	да	
2.4	⇒ изменить содержание персональных данных или другие сведения, затрагивающие интересы личности		нет

	Сумма положительных («Да») ответов по п.2, ∑(«Да») = **$(К_п)_ц$**	2	
3	Может ли задержка в получении защищаемой информации или ее неполучение:		
3.1	⇒ привести к невозможности выполнения взятых организацией обязательств перед третьим лицами	да	
3.2	⇒ привести к несвоевременному принятию решений (или непринятию вообще), важных для практической деятельности организации	да	
3.3	⇒ привести к полной или частичной дезорганизации деятельности организации или ее подразделений	да	
	Сумма положительных («Да») ответов по п.1, ∑(«Да») = **$(К_п)_д$**	3	

По результатам оценки, приведённой в таблице 3, наиболее приоритетными целями ИБ для оцениваемого объекта являются «Конфиденциальность» и «Доступность».

8. Показатели исходной защищенности ИСПДн

Согласно документу ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 4.

Таблица 4 – Показатель исходного уровня защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	-	-	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	-	-	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	-	+	-
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий	-	+	-
локальная ИСПДн, развернутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования	-	-	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	-	+	-
ИСПДн, физически отделенная от сети общего пользования	+	-	-

3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	-	-
запись, удаление, сортировка;	-	+	-
модификация, передача	-	-	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект персональных данных;	-	+	-
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	-	-	+
ИСПДн с открытым доступом	-	-	+
5. По наличию соединений с другими базами персональных данных иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз персональных данных ИСПДн, при этом организация не является владельцем всех используемых баз персональных данных);	-	-	+
ИСПДн, в которой используется одна база персональных данных, принадлежащая организации – владельцу данной ИСПДн	+	-	-
6. По уровню обобщения (обезличивания) персональных данных:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	-	-
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	+	-
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных)	-	-	+
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с персональными данными;	-	-	+
ИСПДн, предоставляющая часть персональных данных;	-	+	-
ИСПДн, не предоставляющая никакой информации.	+	-	-
Итого	29%	57%	14%
	86%		

В результате анализа, представленного в таблице 4, ИСПДн имеет **средний** уровень исходной защищенности (так как не менее 70%

характеристик ИСПДн соответствуют уровню не ниже «средний», а остальные – низкому уровню защищенности).

Уровень защищенности данных для ИСПДн-О определяется в таблице 5.

Таблица 5 – Уровни защищенности персональных данных

Категория ПДн + кол-во	АУ 1 типа	АУ 2 типа	АУ 3 типа
ИСПДн-С более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	УЗ 1	УЗ 1	УЗ 2
ИСПДн-С сотрудников оператора или специальные категории персональных данных менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И данных сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	УЗ 2	УЗ 2	УЗ 4
ИСПДн-О сотрудников оператора или общедоступные ПДн менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	УЗ 2	УЗ 3	УЗ 4

Таким образом, в соответствии с таблицей 5, для ПДн в ЭБС НГУ характерен **уровень защищенности УЗ 2**.

9. Заключение о степени защищенности

Таким образом, для объекта ЭБС НГУ определено:

- класс защищенности ГИС – К3;

В соответствии с классом защищенности ГИС требуется разработать комплекс мер защиты информации (согласно базовому набору, указанному в Приказе ФСТЭК № 17);

- уровень защищенности персональных данных в ИСПДн-О – УЗ 2;

В соответствии с уровнем защищенности ПДн для объекта требуется разработать комплекс мер по обеспечению безопасности персональных данных (согласно приказу ФСТЭК № 21);

- часть объекта относится к КИИ, категория значимости не присвоена;

В соответствии с Постановлением Правительства РФ №127, для объекта КИИ без категории значимости отсутствует необходимость применения дополнительных организационных и технических мер для обеспечения безопасности.

С учётом совокупности выявленных характеристик объекта, также требуется внедрение

- **средств доверенной загрузки (СДЗ) 4 класса** защиты (К3 ГИС + взаимодействие с глобальной сетью + УЗ 2 ИСПДн);
- **средств антивирусной защиты (САЗ) типов «Б» и «В»** (для применения на серверах и на АРМ);
- **средства контроля съемных носителей информации класса 4** (К3 ГИС + взаимодействие с глобальной сетью + УЗ 2 ИСПДн);
- **межсетевых экранов 5 класса** (УЗ 2 ИСПДн);
- **операционных систем типа «А» 5 класса защиты** (общего назначения, для АРМ и серверов + УЗ 2 ИСПДн).