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

ПРАКТИЧЕСКАЯ РАБОТА №7

по дисциплине «Основы информационной безопасности»

Тема: «Оценка структуры факторов риска»

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: провести оценку отношений на множестве факторов риска, расчет профиля риска и определить наиболее значимые факторы.
3. Отчет выполняется с расчетом профиля риска в РискМенеджер - Анализ v3.5 и по методике Вихорева, результаты сравнить.
4. Материал должен содержать титульный лист, постановку задачи, текст и таблицы согласно нормативным документам.

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

1. Оценка структуры факторов риска в соответствии с руководящим документом ФСТЭК

Риск составляют вероятность реализации угрозы и возможный ущерб от этого события.

Методика оценки угроз безопасности информации, утверждённая ФСТЭК, позволяет построить структуру **видов ущерба** (негативных последствий), а также относящихся к ним **субъектов**, **объектов**, **видов воздействия** и **методов реализации**.

Негативные последствия, актуальные для ЭБС НГУ, приведены в таблице 1.

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

№	Виды 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	Ущерб 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

В соответствие с перечисленными в таблице 1 негативными последствиями в таблице 2 указаны объекты воздействия и виды негативного воздействия на них.

Таблица 2 – Объекты воздействия и виды 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)
	Файловый сервер	Несанкционированная модификация, подмена, искажение информации

Публикация недостоверной информации на веб-ресурсах организации (У2)	СУБД	Несанкционированная модификация, подмена, искажение информации

Для определенных видов риска в таблице 3 перечислены виды, категории и уровни возможностей нарушителей.

Таблица 3 – 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; 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	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)

Методы реализации негативного воздействия для указанных видов нарушителей приведены в таблице 4.

Таблица 4 – 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 (H2)	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 (H2)	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 (H1)	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

2. Оценка структуры факторов риска в соответствии с методикой С.В. Вихорева

Методика С.В. Вихорева позволяет описать актуальные **угрозы** ИБ, а также их **источники** и **методы реализации.**

Перечень актуальных угроз безопасности с указанными коэффициентами актуальности $(К_А)_k$ приведён в таблице 5.

Таблица 5 – Актуальные угрозы ИБ для ЭБС НГУ

k	Угрозы ИБ	$(К_А)_k$
1	Хищение (копирование) информации и средств ее обработки	0,22
2	Уничтожение информации и средств ее обработки	0,2
3	Блокирование информации	0,13

Перечень актуальных источников угроз с указанными коэффициентами опасности $(K_{оп})_i$ приведён в таблице 6. Также в таблице представлена информация о показателях: возможности возникновения источников угрозы $(k_1)_i$, готовности источников угрозы $(k_2)_i$ и фатальности применения $(k_3)_i$.

Таблица 6 – Актуальные источники угроз

Код	Источники угроз информационной безопасности	$(k_1)_i$	$(k_2)_i$	$(k_3)_i$	$(K_{оп})_i$
[I.A.2]	потенциальные преступники и хакеры	3	3	4	0,07
[I.B.1]	основной персонал (пользователи, программисты, разработчики)	3	5	4	0,13
[II.A.2]	сети инженерных коммуникации (водоснабжения, канализации)	4	1	2	0,14
[II.B.1]	некачественные технические средства обработки информации	4	4	5	0,10
[II.B.2]	некачественные программные средства обработки информации	5	5	5	0,16
[III.A.1]	пожары	4	5	5	0,10

Перечень актуальных уязвимостей с указанными коэффициентами опасности $(K_{оп})_f$ приведён в таблице 7. Также в таблице представлена информация о показателях: фатальности $(k_1)_f$, удобства $(k_2)_f$ и количества $(k_3)_f$.

Таблица 7 – Актуальные уязвимости

Код	Уязвимости	$(k_1)_f$	$(k_2)_f$	$(k_3)_f$	$(K_{оп})_f$
[A.II.a.4]	аппаратные закладки, устанавливаемые в технических средствах	5	4	5	0,51
[A.II.b.1]	вредоносные программы	5	5	5	0,64
[A.IV.a.1]	отсутствие контролируемой зоны	4	5	4	0,50
[A.IV.a.2]	наличие прямой видимости объектов	4	4	4	0,40
[A.IV.b.2]	использование глобальных информационных сетей	5	5	5	0,78
[A.IV.b.3]	использование арендуемых каналов	3	5	4	0,37
[B.I.a.2]	ошибки при инсталляции и загрузке программного обеспечения	3	4	5	0,39
[B.I.a.3]	ошибки при эксплуатации программного обеспечения	4	5	5	0,66
[B.I.b.1]	ошибки при включении/выключении технических средств	3	5	5	0,50
[B.I.b.3]	ошибки при использовании средств обмена информацией	3	4	3	0,23
[B.I.c.3]	ошибки при организации управления потоками обмена информации	3	4	3	0,23
[B.I.d.2]	повреждение (удаление) данных	5	5	5	0,83
[B.I.d.3]	повреждение (уничтожение) носителей информации	5	4	4	0,53
[B.II.a.2]	нарушения доступа к техническим средствам	5	4	5	0,62
[B.II.a.3]	нарушения соблюдения конфиденциальности	4	4	4	0,39
[C.I.c.1]	сбои операционных систем и СУБД	4	5	4	0,56
[C.I.c.4]	сбои антивирусных программ	4	4	4	0,45

В таблице 8 приведены возможные варианты реализации угроз.

Таблица 8 – Варианты реализации угроз

Источники угроз	Методы реализации	Уязвимости
[I.B.1] - основной персонал (пользователи, программисты, разработчики)	[M2.A.01] - мониторинг (наблюдение) активности каналов связи	[B.II.a.2] - нарушения доступа к техническим средствам
[I.A.2] - потенциальные преступники и хакеры	[M3.B.02] - установка нештатного оборудования или ПО	[B.II.a.2] - нарушения доступа к техническим средствам
[I.B.1] - основной персонал (пользователи, программисты, разработчики)	[M5.A.01] - доступ к носителям информации, техническим средствам	[B.II.a.2] - нарушения доступа к техническим средствам

[I.B.2] - администраторы	[M3.B.02] - установка нештатного оборудования или ПО	[A.II.b.1] - вредоносные программы
[I.B.2] - администраторы	[M3.B.02] - установка нештатного оборудования или ПО	[B.I.d.2] - повреждение (удаление) данных

3. Оценка структуры факторов риска в РискМенеджер – Анализ v3.5

На основании проведённой ранее работы по спецификации исследуемого объекта, при помощи ПО РискМенеджер – Анализ v3.5 для ЭБС НГУ построена модель рисков с оценкой вероятности реализации и ущерба от неё (в тыс. р).

На рисунках 1 и 2 приведён суммарный риск с распределением по структурной модели ЭБС НГУ.

Рисунок 1 – Суммарный риск

	В целом
Название модели: ЭБС и локальная сеть библиотеки НГУ	524,77
Регион: г. Пенза	524,77
ЛС: Библиотека НГУ	524,77
ПС: система ИРБИС	49,50
Объект: ПО "Читатель"	9,90
Объект: ПО "Администратор"	19,80
Объект: ПО "Каталогизатор"	19,80
ПС: ЭБС	475,27
Объект: АРМ читателя	218,18
Объект: АРМ администратора	6,55
Объект: АРМ каталогизатора	6,55
Объект: Сервер БД	27,00
Объект: Марщрутизатор	6,00
Объект: Коммутатор	36,00
Объект: Веб-сервер	95,45
Объект: Файловый сервер	79,55
Объект: Межсетевой экран	0,00

Рисунок 2 – Распределение риска по объектам структурной модели

На рисунке 3 приведено распределение риска по объектам ЭБС (без учёта ИРБИС).

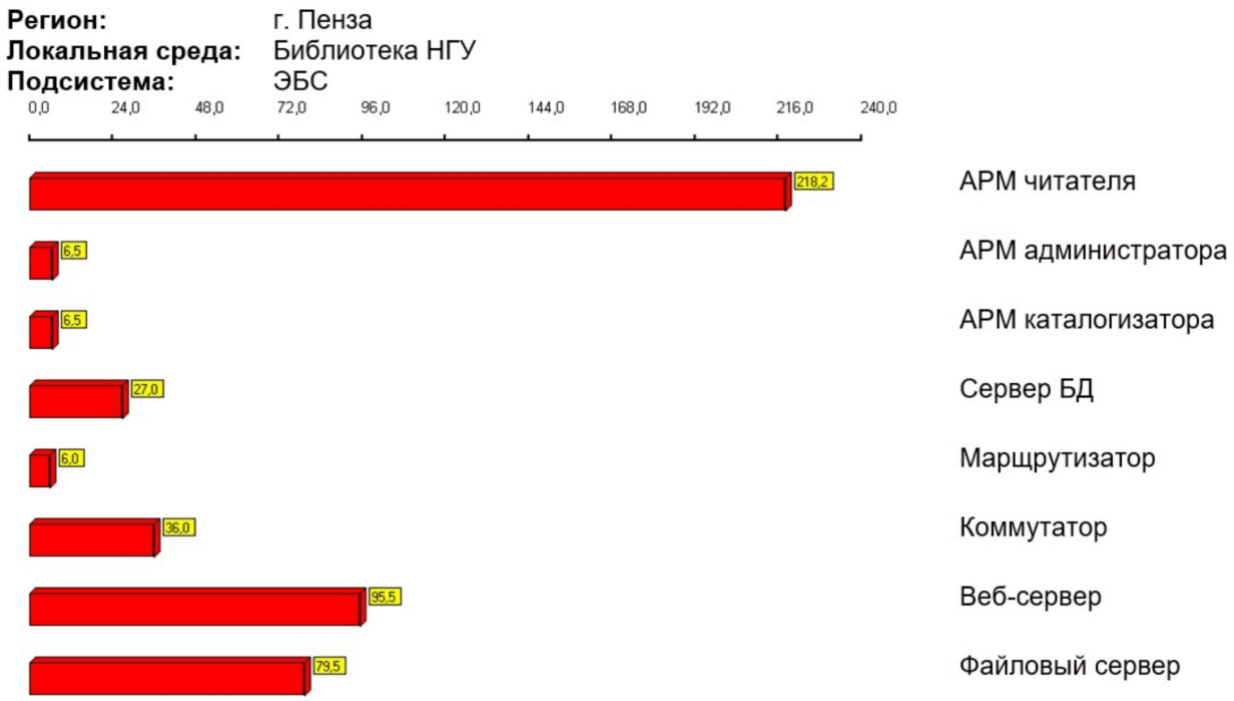

Рисунок 3 – Распределение риска по объектам ЭБС

Из рисунка 3 видно, что объектом с наибольшим риском являются 20 АРМ читателей, находящиеся в читальном зале библиотеки НГУ и принимающие наибольший поток пользователей, далее по убыванию идут Веб-сервер и Файловый сервер как хранилища наиболее ценных данных ЭБС.

4. Выбор комплекса мер защиты в РискМенеджер – Анализ v3.5

На основании построенной ранее модели угроз и проведённой оценки рисков, были сформированы 3 различных по стоимости комплекса мер по защите ЭБС НГУ (рисунок 4).

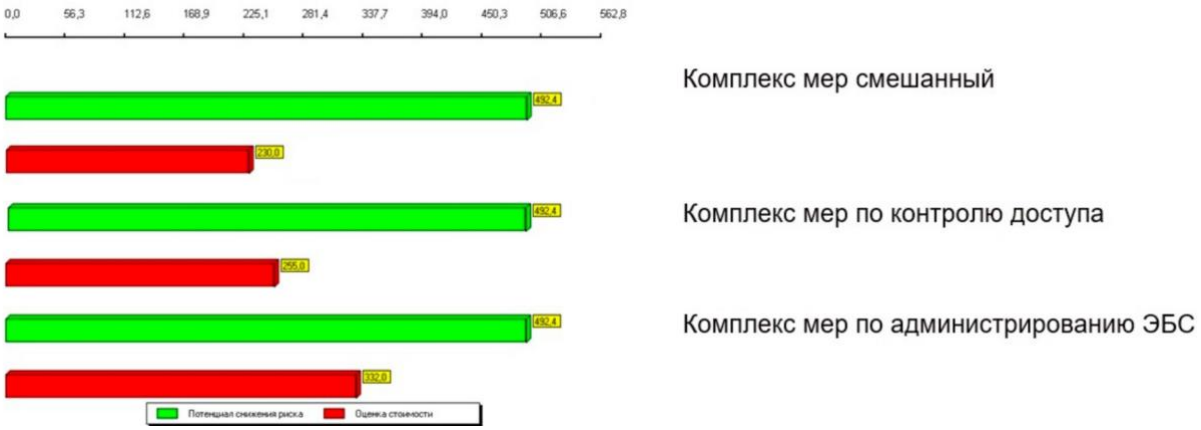

Рисунок 4 – Варианты комплексов мер для ЭБС НГУ

Из рисунка 4 видно, что наиболее выгодным по стоимости является Смешанный комплекс мер.

На рисунке 5 представлено сравнение остаточного риска с исходным риском и условной границей приемлемого для Смешанного комплекса мер.

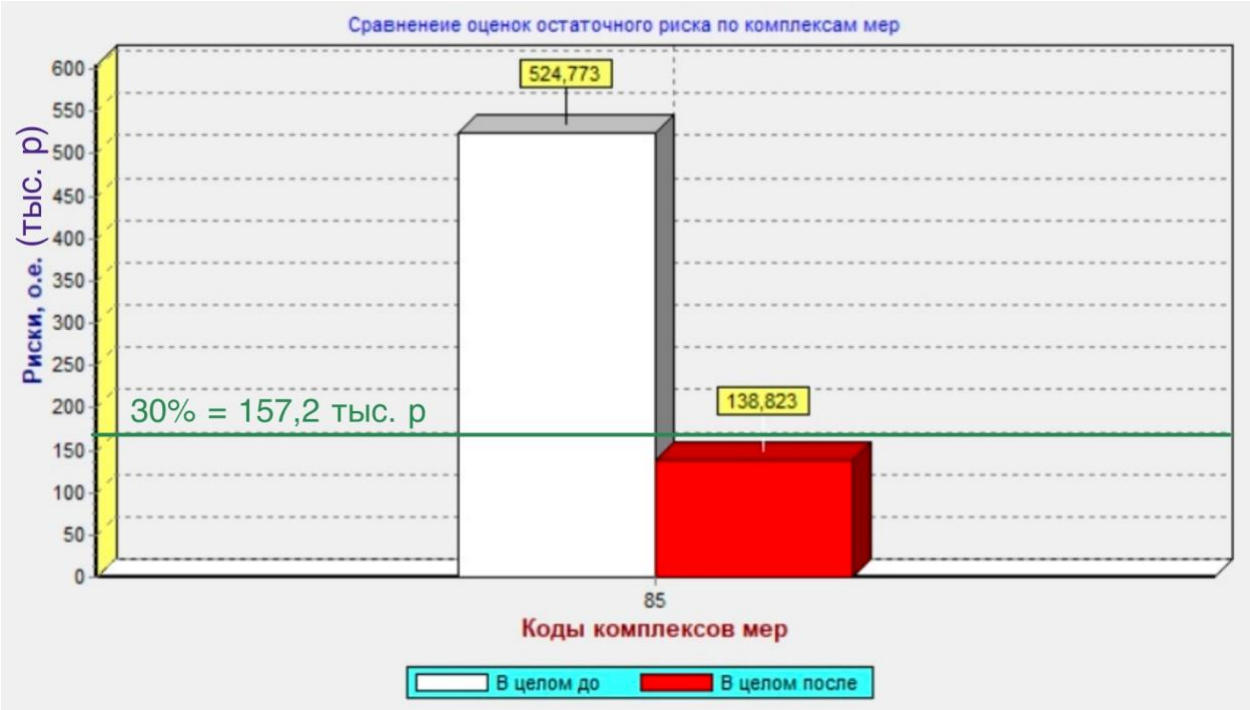

Рисунок 5 – Сравнение остаточного риска с исходным

Из рисунка 5 видно, что Смешанный комплекс мер позволяет снизить оценочный минимум до 138 тыс. рублей. Таким образом, выбранный комплекс мер является эффективным.

5. Выводы

При сравнении рисков, представленных по методике ФСТЭК и методике Вихорева, были описаны:

- ущерб от их реализации;
- источники;
- методы реализации.

Также оценка рисков проведена с помощью ПО РискМенеджер – Анализ v3.5. Для модели ЭБС НГУ предложены три комплекса мер защиты, из которых выбран один наиболее выгодный по стоимости комплекс мер. Для выбранного комплекса мер сделано заключение о его эффективности.