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

ПРАКТИЧЕСКАЯ РАБОТА №8

по дисциплине «Основы информационной безопасности»

Тема: «Разработка и оценка вариантов СЗИ соответственно профилю 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 разработку списка контрмер, дать дополнительные рекомендации по проекту защиты.

3. Отчет выполняется с использованием РискМенеджер - Анализ v3.5.

4. Материал должен содержать титульный лист, постановку задачи, текст и таблицы согласно нормативным документам, а также анализ результативности и эффективности вариантов СЗИ на примере курсовой работы.

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

В предыдущих работах для ЭБС НГУ было 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);

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).

1. Разработка мер защиты информации согласно Приказу ФСТЭК № 17

В предыдущих работах было установлено, что в соответствии с Приказом ФСТЭК №17 «Об утверждении Требований о защите информации,

не составляющей государственную тайну, содержащейся в государственных информационных системах», ЭБС НГУ имеет **класс защищенности ГИС К3**.

Тогда вышеуказанным документом для неё устанавливается базовый набор мер по защите информации и ИС, приведённый в таблице 1 вместе с реализующими меры средствами защиты, планируемыми к внедрению в ЭБС.

Таблица 1 – Меры по защите информации и ИС

ID меры	Меры защиты информации и информационных систем	Средства защиты	Стоимость, р.
1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	мини-ИРБИС32 (3 модуля: «Читатель», «Администратор», «Каталогизатор», до 25 000 пользователей)	49 400
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации		
ИАФ.5	Защита обратной связи при вводе аутентификационной информации		
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)		
2. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	мини-ИРБИС32 (3 модуля: «Читатель», «Администратор», «Каталогизатор», до 25 000 пользователей)	- (указана ранее)
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа		
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	СЗИ Dallas Lock Linux	7 400

УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	мини-ИРБИС32 (3 модуля: «Читатель», «Администратор», «Каталогизатор», до 25 000 пользователей)	- (указана ранее)
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)		
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	СЗИ Dallas Lock Linux	- (указана ранее)
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Континент TLS	290 000
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	СЗИ Dallas Lock Linux	- (указана ранее)
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств		
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)		
3. Ограничение программной среды (ОПС)			
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	СЗИ Dallas Lock Linux (включает СДЗ)	- (указана ранее)
4. Защита машинных носителей информации (ЗНИ)			
ЗНИ.1	Учет машинных носителей информации	СЗИ Dallas Lock Linux (включает СКН)	- (указана ранее)
ЗНИ.2	Управление доступом к машинным носителям информации		
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)		
5. Регистрация событий безопасности (РСБ)			

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	СЗИ Dallas Lock Linux	- (указана ранее)
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации		
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения		
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти		
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе		
РСБ.7	Защита информации о событиях безопасности		
6. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	Kaspersky Endpoint Security для бизнеса Стандартный	20 900
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		
7. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	СКЗ RedCheck (25 лицензий)	5 200
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации		
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе		
8. Обеспечение целостности информационной системы и информации (ОЦЛ)			

ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	СЗИ Dallas Lock Linux	- (указана ранее)
9. Защита среды виртуализации (ЗСВ)			
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	vGate R2 Standard (от 1 до 500 лицензий)	54 000
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин		
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей		
10. Защита технических средств (ЗТС)			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Считыватель "Портал-К" (управление электромагнитными замками для двух дверей: в администраторскую и в серверную)	1960
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены		
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр		
11. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			

ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	Континент TLS	- (указана ранее)
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств		
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе		

2. Разработка мер защиты информации согласно Приказу ФСТЭК № 21

В предыдущих работах было установлено, что в соответствии с Приказом ФСТЭК №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ЭБС НГУ имеет уровень защищенности персональных данных в ИСПДн-О – **УЗ 2**.

Тогда вышеуказанным документом для неё устанавливается базовый набор мер по защите информации и ИС. Большинство пунктов совпадают с таблицей 1, **не вошедшие в неё** приведены в таблице 2 вместе с реализующими меры средствами защиты, планируемыми к внедрению в ЭБС.

Таблица 2 – Меры по защите ПДн

ID меры	Меры защиты информации и информационных систем	Средства защиты	Стоимость, р.
1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	мини-ИРБИС32 (3 модуля: «Читатель»,	- (указана ранее)

		«Администратор», «Каталогизатор», до 25 000 пользователей)	
2. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	СЗИ Dallas Lock Linux	- (указана ранее)
3. Ограничение программной среды (ОПС)			
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	СЗИ Dallas Lock Linux	- (указана ранее)
8. Обеспечение целостности информационной системы и информации (ОЦЛ)			
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Kaspersky Endpoint Security для бизнеса Стандартный	- (указана ранее)
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)		
9. Обеспечение доступности персональных данных (ОДТ)			
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	мини-ИРБИС32 (3 модуля: «Читатель», «Администратор», «Каталогизатор», до 25 000 пользователей)	- (указана ранее)
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала		
10. Защита среды виртуализации (ЗСВ)			
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	vGate R2 Standard (от 1 до 500 лицензий)	- (указана ранее)
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций		
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры		
12. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			

ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	СЗИ Dallas Lock Linux	- (указана ранее)
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных		
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы		
13. Выявление инцидентов и реагирование на них (ИНЦ)			
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Kaspersky Endpoint Security для бизнеса Стандартный	- (указана ранее)
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов		
ИНЦ.3	Своевременное информирование лиц, ответственных инцидентов и реагирование на них, о возникновени информационной системе пользователями и администрато		
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий		
ИНЦ.5	Принятие мер по устранению последствий инцидентов		
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов		
14. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)			
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	мини-ИРБИС32 (3 модуля: «Читатель», «Администратор», «Каталогизатор», до 25 000 пользователей)	- (указана ранее)
УКФ.2	Управление изменениями конфигурации информацион системы защиты персональных данных		
УКФ.3	Анализ потенциального воздействия планируемых конфигурации информационной системы и системы защит данных на обеспечение защиты персональных данных изменений в конфигурации информационной системы лицом (работником), ответственным за обеспечени персональных данных		
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		

Итоговый перечень средств защиты представлен в таблице 3.

Таблица 3 – Итоговый перечень средств защиты

Наименование средства	Комментарий	Цена, р.
мини-ИРБИС32	3 модуля: «Читатель», «Администратор», «Каталогизатор», до 25 000 пользователей	49 400
Континент TLS	До 300 подключений, подключение к TLS серверу в режиме прокси, для безопасного, зашифрованного доступа в Интернет	290 000
Dallas Lock Linux	Для Linux, Система защиты информации (СЗИ), защита от НСД на АРМ в составе сети	7 400
Kaspersky Endpoint Security для бизнеса Стандартный	Под Linux, централизованное управление защитой, контроль программ и устройств	20 900
RedCheck	25 лицензий, система контроля защищенности (СКЗ)	5 200
vGate R2 Standard	от 1 до 500 лицензий	54 000
Считыватель "Портал-К"	Управление электромагнитными замками для двух дверей: в администраторскую и в серверную	1 960
Итого		428 860

3. Выводы

В результате классификации по классу защищенности ГИС и уровню защищенности ИСПДн, в соответствии с перечнями мер, указанными в Приказах ФСТЭК № 17 и № 25, для ЭБС НГУ был разработан комплекс мер защиты информации и представлен список средств защиты. Для средств защиты рассчитана их суммарная стоимость – 428 860 рублей.