



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«МИРЭА – Российский технологический университет»
РТУ МИРЭА**

Институт искусственного интеллекта
Базовая кафедра №252 – информационной безопасности

ПРАКТИЧЕСКАЯ РАБОТА

По дисциплине
«Техническая защита информации»

Тема практической работы
«Построение защищённой системы "Библиотека" >

Студенты группы ККСО-03-19

Николенко В.О.
Воеводин К.А.
Шарилов А.С.
Даваев В.П.
Лантаев М.М.
Носов Г.А.

Руководитель практической работы Близнецов М. С.

(подпись)

Москва – 2023

СОДЕРЖАНИЕ

1. Условия задания	3
2. Словарь терминов и слэнговых выражений	4
3. Блок-схема «Защищаемая информация»	5
4. Схемы защищаемого объекта	6
5. Личности работников с допуском. Персональная информация.	10

1. УСЛОВИЯ ЗАДАНИЯ

Вариант 4: Библиотека.

1. Состоит из 3 корпусов (административный, операционный, архивный).

2. Все объекты размещены на 1 улице, имеют каждый свою собственную зону безопасности, также имеют сообщения по улицам личного пользования и по туннелям служебного пользования расположенным под землёй.

3. Администрация имеет доступ только к коммерческой информации о деятельности библиотеки.

4. До 2153 года библиотека была объектом общего пользования и не содержала никаких секретных данных.

5. Информационные материалы в библиотеке представлены как на бумажных носителях, так и в электронной форме, в т.ч. посредством доступа в интернет.

6. Приняты следующие решения в отношении библиотеки:

а. Передать на хранение документальные материалы со спец. доступом "а" и "б" формы.

б. Создать инфраструктуру позволяющую проводить хранение, учёт и работу с документами уровня доступа до "б" формы включительно.

с. Весь предыдущий функционал библиотеки сохраняется.

д. Материалы со спец. доступом "б" формы предлагается хранить на бумажных носителях и работать с ними только в пределах спец. помещений библиотеки.

е. Материалы со спец. доступом "а" формы предлагается хранить как на бумажном так и на электронных носителях (но не одновременно), при этом по возвращении необходимо предусмотреть проверку подлинности.

ф. Работа с документами происходит только в операционном корпусе, хранение - только в архивном.

г. Администрация, главные инженеры корпусов и глава секции информатизации должны получить доступ по форме "б", а также рабочие места, оснащённые ПЭВМ для работы с документами по "а" спец. доступу.

2. СЛОВАРЬ ТЕРМИНОВ И СЛЭНГОВЫХ ВЫРАЖЕНИЙ

ПЭМИН – побочное электромагнитное излучение и наводки. Различного вида побочные электромагнитные излучения (ЭМИ) технических средств передачи информации (ТСПИ).

Зашумление – это процесс добавления случайного или нежелательного сигнала, известного как шум, к сигналу или данным, с целью усложнить или исказить их интерпретацию или использование. Зашумление может быть использовано как метод защиты информации, создания секретности, а также для снижения эффективности анализа или восстановления оригинального сигнала.

Шумогенераторы – это устройства или программные алгоритмы, предназначенные для создания и генерации шума. Шумогенераторы создают случайные или псевдослучайные сигналы различных частот и амплитуд, которые могут быть использованы для зашумления.

Экранирование – это процесс создания физической или электрической барьерной структуры, предназначенной для блокирования или снижения проникновения электромагнитных полей, сигналов или излучений внутрь или изнутри определенной области. Экранирование может использоваться для защиты от помех, подавления электромагнитных излучений, обеспечения конфиденциальности или предотвращения несанкционированного доступа к информации.

Помехоподавляющие фильтры – к ним относятся фильтры нижних и верхних частот, полосовые, заграждающие и т.п. Основное назначение фильтров - пропускать сигналы с частотами, лежащими в заданной полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы. Для исключения просачивания информационных сигналов в цепи электропитания используются фильтры нижних частот, которые пропускают сигналы с частотами ниже граничной частоты и подавляют - с частотами выше граничной частоты.

3. БЛОК-СХЕМА «ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ»

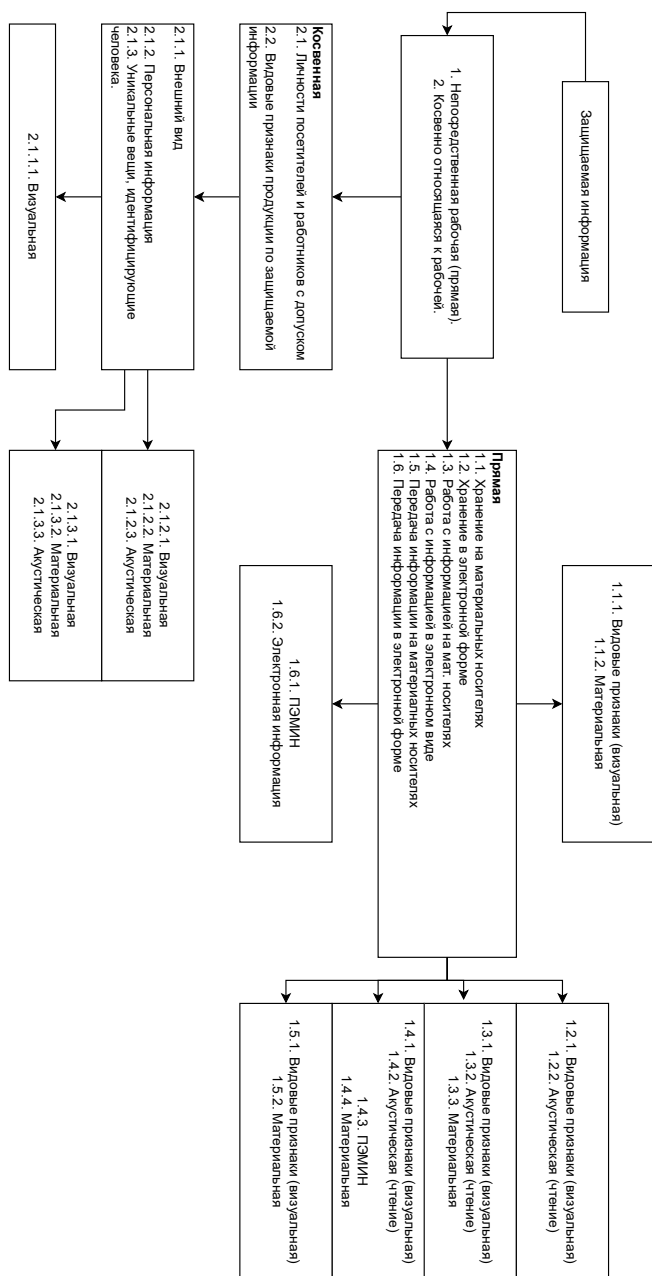


Рис. 1: Графическая иллюстрация типов защищаемой информации на разных уровнях.

Наземный этаж

Главный вход

СТОЛ

СТОЛ

3.15 м²

Дверь с пропускной системой

Дверь в стене с пропускной системой

14.18 м²

КНИЖНЫЕ ПОЛКИ

КНИЖНЫЕ ПОЛКИ

Винтовая лестница на подземный этаж

6

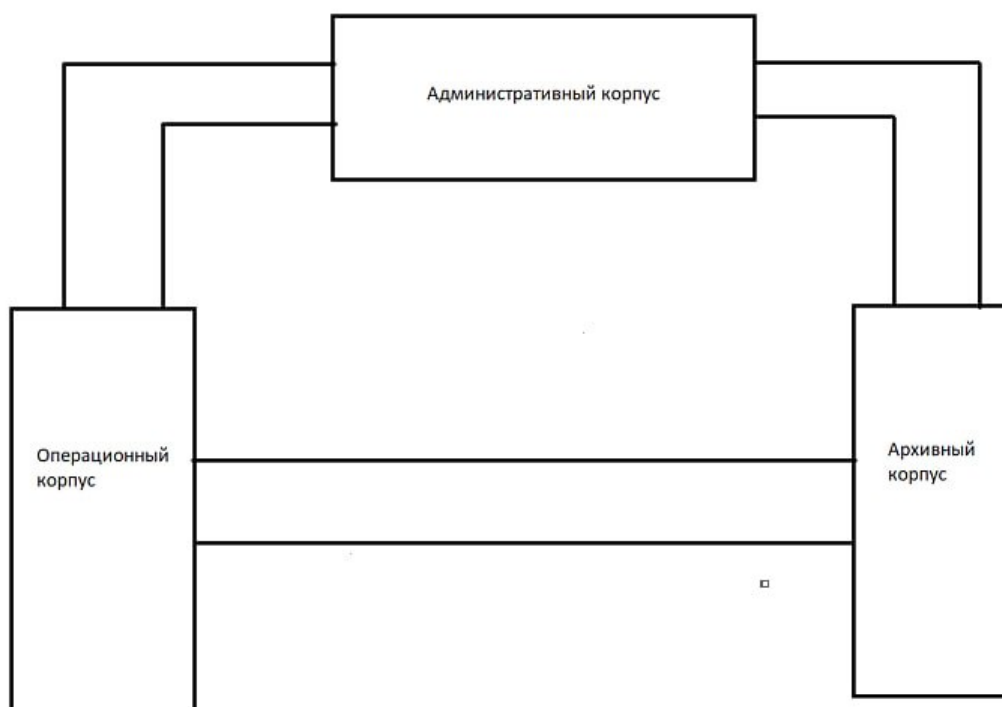


Рис. 3: Графическая иллюстрация расположение корпусов и подземных переходов.

1.1. Работа с документами допуска "б" осуществляется в специально оборудованных помещениях с видеонаблюдением и контрольно-пропускной системой.

1.2. На входе в каждое помещение осуществляется полный досмотр лицами, которые отвечают за охрану помещений и имеют допуск уровня «б» или выше.

1.3. Помещения располагаются в подвальной части здания (не имеют окон) и оборудованы шумоизоляцией и устройствами шумогенерации.

1.4. Для работы с информацией допуска «б» в разных корпусах здания оборудованы специальные закрытые подземные переходы с собственной отдельной вентиляцией.

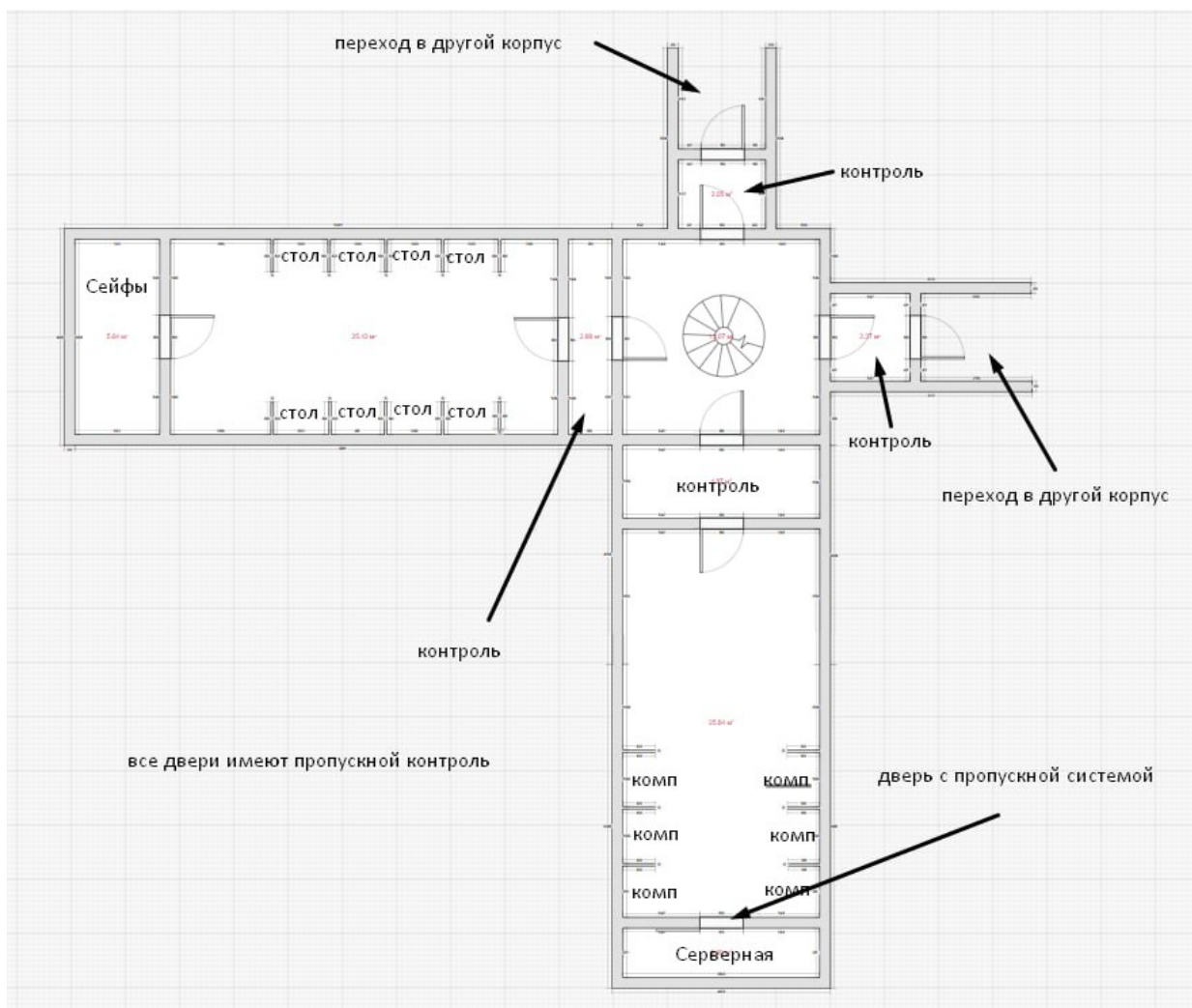


Рис. 4: Графическая иллюстрация подвального помещения.

2.1. В каждом корпусе рядом со спец помещениями оборудованы специальные закрытые серверные комнаты, в которых хранится информация с камер видеонаблюдения в спец помещениях, электронные копии документов допуска «а» и сведения о перемещениях всех сотрудников и посетителей.

2.2. Подвальные спец помещения оборудованы дренажной системой с насосом, имеющей отдельные водоотводы обособленно от канализации в целях безопасности.

2.3. Материалы со спец допуском «б» хранятся в закрытом помещении в бумажном виде. Работа с ними производится строго в этом помещении.

2.4. Каждый пакет документов хранится в отдельной бумажной непрозрачной папке.

2.5. Документы распределены по металлическим ячейкам, оборудованным электронными замками.

2.6. После работы с документами необходимо вернуть их на исходное место (в отведенные ячейки)

2.7. При отключении электричества - все электронные замки на ячей-

ках внутри и на входной двери - закрываются без возможности открыть до включения питания.

2.8. Специально оборудованные помещения имеют отдельную закрытую вентиляционную систему.

ПЭМИН

3.1. Экранирование помещения. Помещение должно быть защищено от электромагнитных излучений с помощью специальных материалов, таких как фольга или металлическая сетка. Это позволит снизить уровень электромагнитных наводок и помешает получить доступ к данным.

3.2. Защита кабелей и сетей. Кабели и сети должны быть защищены от электромагнитных наводок с помощью экранирования и использования специальных фильтров. Это позволит снизить вероятность утечки данных через ПЭМИН.

Хранение и использование документов в электронной форме.

4.1.1. В электронном виде хранятся исключительно материалы со спец допуском «а».

4.1.2. Хранение электронной формы на закрытом сервере.

4.1.3. Доступ к информации происходит только со специально оборудованных ПЭВМ администрации и главных инженеров путем включения в локальную сеть без доступа в интернет.

4.1.4. ПЭВМ оборудованы таким образом, что невозможно подключить/снять какие-либо информационные накопители. Пользователь может только читать информацию через защищенное приложение.

4.1.5. Данные о каждом входе в приложение сохраняются на защищенном сервере.

4.1.6. Помещения Администрации, главных инженеров корпусов и главы секции информатизации в которых устанавливаются ПЭВМ оборудованы на входе электрическим замком, открыть который можно только персональными ключ-картами. Замки надежно закрываются автоматически при закрытии двери.

4.1.7. Администрация, главные инженеры корпусов и глава секции информатизации имеют допуск «б» и оснащенные места с ПЭВМ для работы с документами допуска «а».

Хранение и использование документов допуска "а" в бумажном виде.

4.2.1. Все бумажные версии материалов со спец.допуском «а» должны храниться в запираемых шкафах или сейфах.

4.2.2. Доступ к документам осуществляется в специально отведенные дни и часы.

5. ЛИЧНОСТИ РАБОТНИКОВ С ДОПУСКОМ. ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ.

5.1. Помещения оборудованы системой электронных пропусков. Каждый пропуск представляет из себя личную карту с данными её владельца и уровнем допуска.

5.2. Для доступа в личный кабинет (в случае работников и администрации) и доступа к документам допуска уровня «б» необходим электронный пропуск.

5.3. На закрытый сервер поступают данные о перемещении и взаимодействии с конкретными ячейками всех пользователей электронных пропусков.

5.4. В случае утраты пропуска одного из сотрудников/посетителей, он сразу блокируется и выпускается новый.

5.5. Запрещено проносить в спец помещение любые носители информации.

5.6. Косвенная информация, касающаяся личных данных работников, уровень их допуска, подробной статистики их посещений и передвижений внутри корпусов, хранится в отдельных каталогах на защищенном сервере.

5.7. Персонал, имеющий допуск и работающий в закрытых секторах, не имеет какой-либо специальной формы и других отличительных особенностей.

5.8. Доступ к информации по посетителям библиотеки с формами допуска "а" и "б" имеют работники библиотеки с допусками формы "а" и "б" соответственно, притом персонал с допуском по форме "б" может работать с посетителями с допуском по форме "а" и без допуска вовсе, так же как "а" может работать с простыми посетителями.

5.9. Информация по посетителям библиотеки с формами допуска хранится (а также обрабатывается и читается) на тех же ПЭВМ, что и информация по остальным пользователям, но для доступа требуется персональная ключ-карта сотрудника с определённой формой допуска, описанной в п. 5.8.

Защита косвенной информации помимо персонала.

5.1.1. Отсутствие прямых вывесок с указанием закрытых секций.

5.1.2. С пользователями защищаемых документов обсуждение происходит внутри защищённого помещения.

5.1.3. Двери в закрытые секции закрыты электронными замками, оборудованы доводчиками.