

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

***«Инженерно-технические средства защиты
информации»***

На тему:

**«Проектирование инженерно-технической системы защиты информации на
предприятии»**

Выполнил:

Студент группы N34491

Юзев Артём

Максимович



Проверил преподаватель:

Попов Илья Юрьевич,

доцент ФБИТ, к. т. н.

Отметка о выполнении:

Санкт-Петербург

2023 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Юзев А.М.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю., доцент, к. т. н.

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

Задание Цель: спроектировать инженерно-техническую систему защиты информации на предприятии. Задачи: 1. Выделить организационную структуру предприятия.

2. Обосновать защиту информации. 3. Рассмотреть план предприятия. 4. Провести анализ рынка.

5. Разработать итоговый план предприятия.

Краткие методические указания

Содержание пояснительной записки

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент

27 октября 2023

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Юзев А.М.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю., доцент, к. т. н.

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение титульных листов и поиск источников	29.09.2023	30.09.2023	
2	Анализ информации	29.09.2023	30.09.2023	
3	Написание курсовой работы	14.10.2023	14.10.2023	
4	Подготовка презентации	21.10.2023	21.10.2023	
5	Защита курсовой работы	28.10.2023	28.10.2023	

Руководитель

(Подпись, дата)

Студент



27 октября 2023

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент Юзев А.М.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации)

Руководитель Попов И. Ю., доцент, к. т. н.

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА
(РАБОТЫ)**

1. Цель и задачи
работы

☒ Предложены студентом

☐ Сформулированы при участии студента

☐ Определены руководителем

2. Характер
работы

☐ Расчет

☐

☐ Моделирование

Конструирование

Другое: Исследовательская
работа

3. Содержание работы

В ходе работы мы познакомимся с рынком инженерно-технических средств защиты информации а также разработаем инженерно-техническую систему защиты информации

4. Выводы

В результате выполнения курсовой работы я спроектировал инженерно-техническую систему защиты информации для предприятия «Энигма». Также научился выделять организационную структуру, провёл анализ рынка решений, а также разработал итоговый план предприятия.

Руководитель

(Подпись, дата)

Студент

27 октября 2023

(Подпись, дата)

«27» октября 2023 г.

Содержание

ВВЕДЕНИЕ	6
1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ.....	7
2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ	8
3. РАССМОТРЕНИЕ ПЛАНА	16
4. АНАЛИЗ РЫНКА	17
5. ИТОГОВЫЙ ПЛАН ПРЕДПРИЯТИЯ.....	26
ЗАКЛЮЧЕНИЕ	27
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	28

Введение

Целью данной работы является проектирование инженерно-технической системы защиты информации на предприятии

Для достижения поставленной цели необходимо выполнить следующие задачи:

- выделить организационную структуру предприятия;
- обосновать защиту информации;
- рассмотреть план предприятия;
- провести анализ рынка;
- разработать итоговый план предприятия.

1. Организационная структура предприятия

Для проектирования инженерно-технической системы защиты информации на предприятии мы должны провести анализ общих сведений данного предприятия.

Наименование организации: «Энигма»

Область деятельности: Разработка специализированного программного обеспечения для ведения секретных операций и сбора разведывательной информации.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа: Рисунок 1

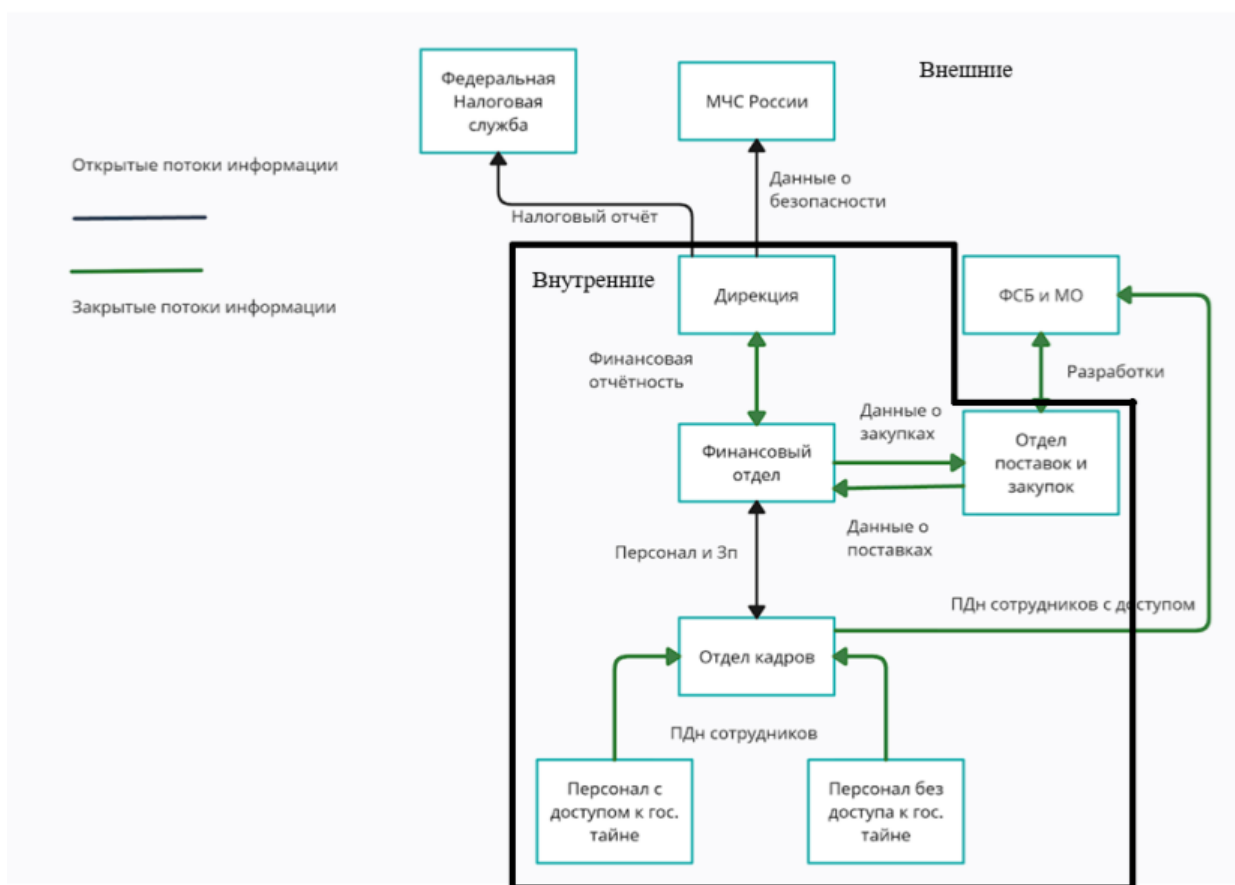


Рисунок 1 – Основные информационные процессы и потоки в организации

2. Обоснование защиты информации

Для обоснования защиты информации мы проведём анализ существующих РПД. Так как наше предприятие работает с государственной тайной, то рассмотрим документы, которые относятся к гос тайне.

1.Законы Российской Федерации:

«О государственной тайне» от 21 июля 1993 г. N 5485–1 (последняя редакция).

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Государственную тайну составляют:

1. сведения в военной области:

- о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
- о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2. сведения в области экономики, науки и техники:

- о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;
- об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства
- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
- о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

Статья 30. Контроль за обеспечением защиты государственной тайны

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах

полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

2.Указы Президента Российской Федерации:

«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.

В соответствии со статьей 4 Закона Российской Федерации "О государственной тайне" постановляю:

1. Утвердить прилагаемый перечень сведений, отнесенных к государственной тайне.
2. Правительству Российской Федерации организовать работу по приведению действующих нормативных актов в соответствие с перечнем сведений, отнесенных к государственной тайне.
3. Настоящий Указ вступает в силу со дня его подписания.

«О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108.

В соответствии с Законом Российской Федерации "О государственной тайне" постановляю:

1. Образовать Межведомственную комиссию по защите государственной тайн

«Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

В целях дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти постановляю:

Утвердить прилагаемый перечень сведений конфиденциального характера.

3.Постановления Правительства Российской Федерации:

Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921-51.

Настоящее Положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну.

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства РФ.

Защита осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путём проведения специальных работ, порядок организации и выполнения которых определяется Правительством РФ

Главными направлениями работ по защите информации являются:

- Обеспечение эффективного управления системой защиты информации
- Определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения
- Анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технически каналов утечки сведений, подлежащих защите
- Разработка организационно-технических мероприятий по защите информации и их реализация
- Организация и проведение контроля состояния защиты информации

Основными организационно-техническими мероприятиями по защите информации являются:

- Лицензирование деятельности предприятий в области защиты информации
- Аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности
- Сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам
- Введение территориальных, частотных, энергетически, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите
- Создание и применение информационных и автоматизированных систем управления в защищенном исполнении

– Разработка и внедрение технических решений и элементов защиты информации при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи

– Разработка средств защиты информации и контроля за её эффективностью (специального и общего применения) и их использование

– Применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи

«О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. №333.

В соответствии с Законом Российской Федерации "О государственной тайне" и в целях установления порядка допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, Правительство Российской Федерации постановляет:

1. Утвердить Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны (прилагается).

3. Федеральной службе безопасности Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Службе внешней разведки Российской Федерации совместно с заинтересованными министерствами и ведомствами Российской Федерации в 3-месячный срок разработать комплекс мер организационного, материально-технического и иного характера, необходимых для осуществления лицензирования деятельности предприятий, организаций и учреждений по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

4. Установить, что предприятия, учреждения и организации, допущенные к моменту принятия настоящего постановления к работам, связанным с использованием

сведений, составляющих государственную тайну, могут осуществлять эти работы в течение 1995 года.

7. Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (далее именуются - руководители предприятий), и при выполнении следующих условий:

- соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
- наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;
- наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

«О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. №513.

В связи с созданием в Министерстве обороны Российской Федерации системы сертификации средств защиты информации, предусмотренной постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (Собрание законодательства Российской Федерации, 1995, N 27, ст. 2579), Правительство Российской Федерации постановляет :

Дополнить абзац третий пункта 2, абзацы второй и пятый пункта 10 Положения о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, утвержденного постановлением Правительства Российской Федерации от 15 апреля 1995 г. N 333 (Собрание законодательства Российской Федерации, 1995, N 17, ст. 1540; 1996, N 18, ст. 2142), после слов: "Служба внешней разведки Российской Федерации" словами: "Министерство

обороны Российской Федерации".

«Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870.

1. Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

2. Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

3. К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из указанных областей.

4. К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

5. К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-разыскной области деятельности.

«О сертификации средств защиты информации» от 26 июня 1995 г, №608.

В соответствии с Законами Российской Федерации "О государственной тайне" и "О сертификации продукции и услуг" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемое Положение о сертификации средств защиты информации.

2. Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Федеральной службе безопасности Российской Федерации и Министерству обороны Российской Федерации в пределах определенной

законодательством Российской Федерации компетенции в 3-месячный срок разработать и ввести в действие соответствующие положения о системах сертификации, перечни средств защиты информации, подлежащих сертификации в конкретной системе сертификации, а также по согласованию с Министерством финансов Российской Федерации порядок оплаты работ по сертификации средств защиты информации.

1. Настоящее Положение устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам (далее именуется - система сертификации).

Системы сертификации создаются Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (далее именуются - федеральные органы по сертификации).

3. Рассмотрение плана

В данном разделе мы проанализируем план предприятия (рисунок 2)

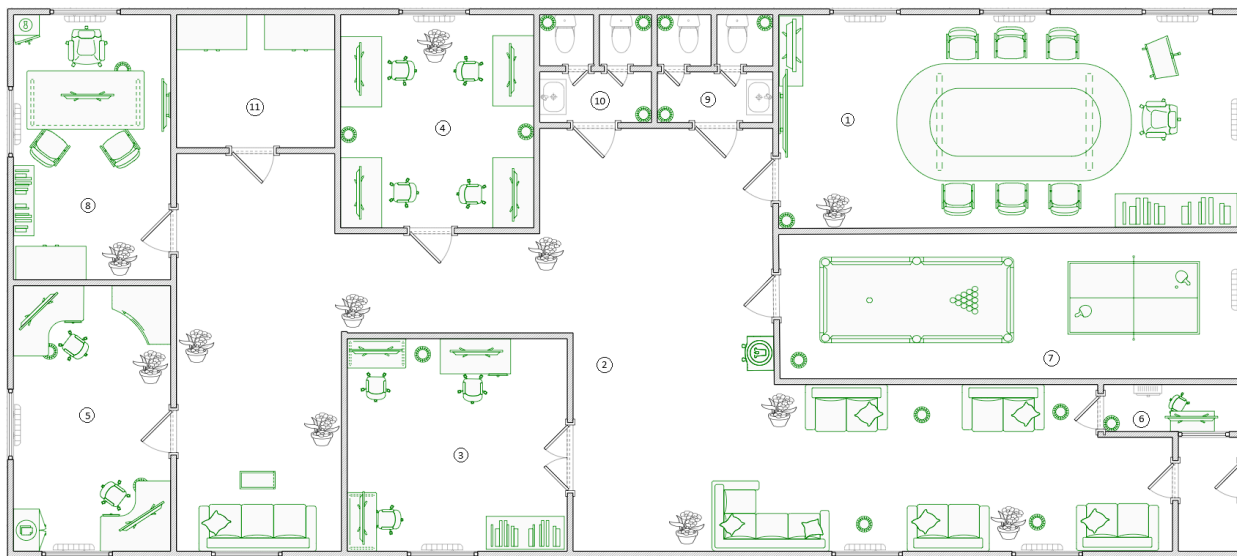


Рисунок 2 – План предприятия

Легенда:

1. Переговорная - кабинет для переговоров, где может обрабатываться информация, относящаяся к гос. тайне.
2. Коридор
3. Комната для сбора и анализа секретных сведений (есть гос. тайна)
4. Комната для разработки специализированного ПО (есть гос. тайна)
5. Кабинет Бухгалтера и отдела поставок и закупок (есть гос. тайна)
6. Кабинет охраны
7. Игровая для поднятия настроения
8. Кабинет Директора (есть гос. тайна)
9. Женский туалет
10. Мужской туалет
11. Серверная

4. Анализ рынка

В данном разделе произведем анализ рынка решений по инженерно-технической защите информации.

Выберем подходящие решения, которые подходят к нашим каналам утечки и напомним им описание.

1. Блокираторы беспроводной и сотовой связи:

- Блокираторы беспроводной связи предназначены для блокирования работы устройств несанкционированного получения информации, работающих в стандартах сетей сотовой связи и в стандартах Bluetooth и WiFi.

- Принцип работы заключается в генерации шумовой помехи в необходимом диапазоне частот. При этом возможна плавная регулировка мощности помехового сигнала в каждом из диапазонов, что позволяет обеспечить блокирование беспроводных стандартов связи только в границах защищаемого помещения.

- Защита является активной.

2. Акустическое зашумление:

- Система постановки акустических помех предназначена для противодействия специальным средствам несанкционированного съема информации, использующим в качестве канала утечки воздушную среду помещения. К ним относятся: микрофоны и диктофоны.

- Защита является активной.

3. Виброакустическое зашумление:

- Система постановки виброакустических помех предназначена для противодействия специальным средствам несанкционированного съема информации, использующим в качестве канала утечки ограждающие конструкции помещения. К ним относятся:

- Электронные или акустические стетоскопы для прослушивания через потолки, полы и стены
- Проводные или радиомикрофоны, установленные на ограждающие конструкции или водопроводные и отопительные трубопроводы;
- Лазерные или микроволновые системы съема информации через оконные проемы помещений.

4. Защита сети 220/380В:

- Сети переменного тока содержат в себе двойную опасность. Во-первых, это утечка акустической информации по сети переменного тока (220 В). Во-вторых, угроза утечки информативных сигналов средств оргтехники.

- Существуют пассивные и активные методы защиты сети переменного тока (220 В) от несанкционированного съема информации.

- Пассивная защита сети 220 В заключается в использовании сетевых помехоподавляющих фильтров. Такие фильтры не пропускают информативные сигналы, возникающие при работе средств оргтехники. Причём, правильно установленный фильтр также защищает средства оргтехники от вредного влияния внешних помех. Следует учитывать, что для эффективной работы помехоподавляющих фильтров необходимо качественное заземление.

- К активным методам защиты сети переменного тока (220 В) относятся методы, предусматривающие формирование специальными генераторами шумового сигнала, превосходящего по уровню сигналы устройств съёма информации или информативные сигналы.

5. Пространственное зашумление:

- При работе самых различных устройств (например, вычислительной техники) могут появляться сигналы ПЭМИН (побочные электромагнитные излучения и наводки), содержащие обрабатываемую информацию конфиденциального характера. Эти сигналы могут быть перехвачены с помощью специальной аппаратуры.

- Генераторы радиопомех предназначены для работы в составе систем активной защиты информации (САЗ), обеспечивая защиту информации от утечки по каналам ПЭМИН путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта.

- Защита является активной.

6. Защита слаботочных линий и линий связи:

- Слаботочных линий и линий связи содержат в себе угрозу утечки акустической информации по ним. Устройства оказывают противодействие прослушиванию/расшифровке переговоров.

- Защита является пассивной.

Теперь проанализируем рынок (таблица 2) исходя из наших решений

Таблица 2 – Анализ рынка

Категория	Наименование устройства	Краткое описание	Цена
Блокираторы беспроводной и сотовой связи:	ЛГШ-718	Блокиратор сотовой связи ЛГШ-718 предназначен для блокировки (подавления) связи между базовыми станциями и мобильными телефонами сетей сотовой связи, работающих в стандартах: IMT-MC-450, GSM900, DSC/GSM1800, (DECT1800), IMT-2000/UMTS (3G), 4G-2600 (LTE, WiMAX), Bluetooth, WiFi. Эффективный радиус подавления 3.50 м	114400руб.
	ЛГШ-715	Блокиратор беспроводной связи стандартов IMT-MC-450, GSM900, DSC/GSM1800, (DECT1800), IMT-2000/UMTS (3G) Эффективный радиус подавления 3.50 м	74620 руб.
	ЛГШ-701	Блокиратор сотовой связи стандартов: IMT-MC-450 GSM900 DSC/GSM1800 Эффективный радиус подавления 3.50 м	97500
Акустическое зашумление:	ЛГШ-404	- Сертифицирован ФСТЭК России по 2 классу защиты - Возможность установки в ВП до 2 категории включительно	35100 руб.

		- Возможность подключения до 40 преобразователей	
	ЛГШ-303	Изделие «ЛГШ-303» мобильно и предназначено для работы в помещениях, (автомобилях) и других местах не требующих стационарных средств защиты информации по прямому акустическому каналу и не оборудованных стационарными источниками питания.	15600
	ЛГШ-304	Изделие «ЛГШ-304» соответствует: - типу «Б» средства акустической защиты информации с активным (содержащим в своей конструкции индивидуальный задающий источник шума) преобразователем, питаемым по линии вторичного электропитания от центрального блока питания. Изделие «ЛГШ-304» соответствует требованиям «Требования к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) – по 2 классу защиты.	25 220 руб.

Виброакустическое зашумление:	ЛГШ-404	- Сертифицирован ФСТЭК России по 2 классу защиты - Возможность установки в ВП до 2 категории включительно - Возможность подключения до 40 преобразователей	35100 руб.
	ЛГШ-402	Изделие «ЛГШ-402» соответствует типу «А» - средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными (не содержащими в своей конструкции индивидуальные задающие источники шума требующие электропитания) преобразователями.	18200 руб.
Защита сети 220/380В:	ЛГШ-221	Изделие «ЛГШ-221» является средством активной защиты информации (тип Б) от утечки за счет наводок информативного сигнала на цепи заземления и электропитания, выходящие за пределы контролируемой зоны. Изделие «ЛГШ-221» соответствует требованиям по безопасности информации, установленным в документе «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) –	36400 руб.

		по 2 классу защиты, может применяться в выделенных помещениях до 2 категории включительно.	
	ЛППФ-40-1Ф	Сетевой помехоподавляющий фильтр «ЛППФ-40-1Ф» является средством пассивной специальной защиты технических средств от утечки информации за счет наводок, т.е. преобразования излучения технических средств в электрический сигнал в сети электропитания, выходящей за пределы контролируемой зоны. Предельное значение тока, при котором допускается эксплуатация изделия 40 А	70200 руб.
Пространственное зашумление	ЛГШ-501	Изделие «ЛГШ-501» является: - средством активной защиты информации от утечки за счет побочных электромагнитных излучений (тип «А»); - средством активной защиты информации от наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.	29900 руб.
	ЛГШ-516СТАФ	Изделие «ЛГШ-516СТАФ» соответствует 2 классу защиты.	51000 руб.

		Изделие «ЛГШ-516СТАФ» соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) с учетом изменений, внесенных приказом ФСТЭК России № 028 от 28.11.2019.	
	ЛГШ-503	Изделие «ЛГШ-503» является: - средством активной защиты информации от утечки за счет побочных электромагнитных излучений (тип «А»); - средством активной защиты информации от наводок информативного сигнала на проводники, в том числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.	44200 руб.
	ЛГШ-513	Изделие «ЛГШ-513» соответствует: - типу «А» - средства активной защиты информации от утечки за счет побочных электромагнитных излучений; - типу «Б» - средства активной защиты информации от утечки за счет наводок информативного сигнала на проводники, в том	39000 руб.

		<p>числе на цепи заземления и электропитания, токопроводящие линии и инженерно-технические коммуникации, выходящие за пределы контролируемой зоны.</p> <p>Изделие «ЛГШ-513» соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты.</p>	
Защита слаботочных линий и линий связи	Гранит-8	Назначение фильтра пропускать сигналы в речевом диапазоне частот при нормальном режиме работы телефонной линии и ослаблять высокочастотные сигналы, которые могут подаваться в линию при высокочастотном навязывании.	4160 руб.
	ЛУР-2	Размыкатель слаботочных линий питания	5590
	ЛУР-4	Размыкатель слаботочных линий Телефон	
	ЛУР-8	Размыкатель слаботочных Ethernet	

По результатам анализа рынка я выбрал такие средства защиты:

1. Блокираторы беспроводной и сотовой связи: ЛГШ-701 (Так как он единственный имеет сертификат ФСТЭК)
2. Акустическое зашумление: ЛГШ-404 (Так как он имеет сертификат ФСТЭК, и умеет в виброакустическое зашумление)

3. Виброакустическое шумление: ЛГШ-404 (Так как он имеет сертификат ФСТЭК, и умеет в акустическое шумление)
4. Защита сети 220/380В: Средством активной защиты будет являться ЛГШ-221, а в качестве пассивной защиты ЛППФ-40-1Ф.
5. Пространственное шумление: ЛГШ-516СТАФ (Так как он имеет сертификат ФСТЭК)
6. Защита слаботоочных линий и линий связи: ЛУР-2,ЛУР-4,ЛУР-8 все они входят в состав ЛГШ-404

5. Итоговый план предприятия

В данном разделе мы спроектировали инженерно-техническую систему защиты информации на предприятии «Энигма» (рисунок 3).

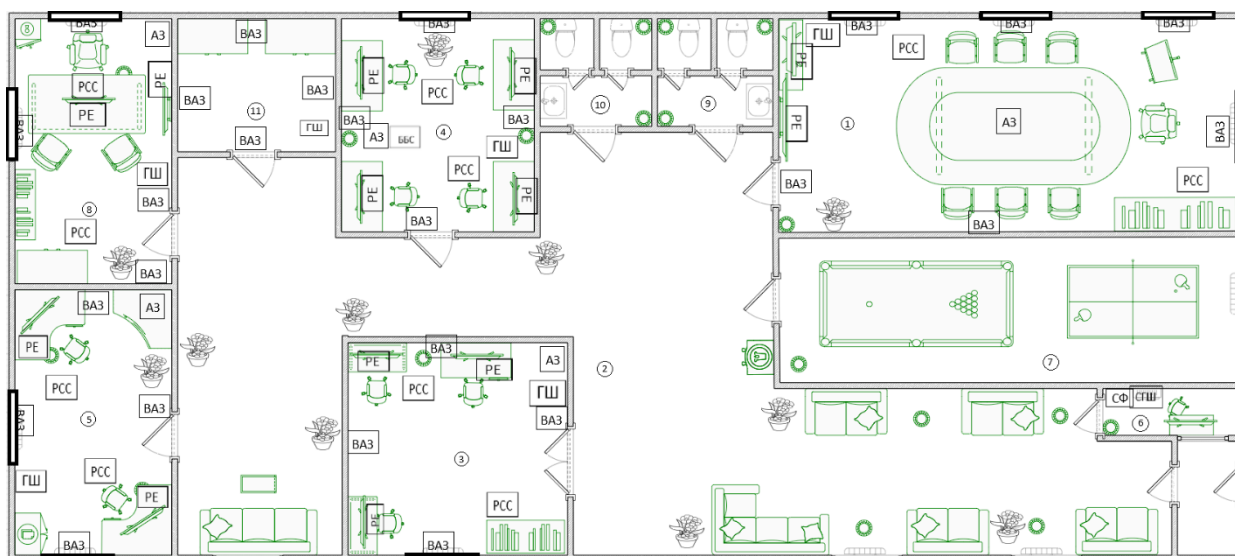



Рисунок 3 – Инженерно-техническая система защиты информации

Легенда:

- АЗ - Система акустических помех;
- ББС - Блокиратор беспроводной связи;
- ВАЗ - Система постановки виброакустических помех;
- ГШ - Генератор шума ПЭМИ;
- РСС - Размыкатель слаботочных сетей;
- РЕ - Размыкатель Ethernet;
- СГШ - Сетевой генератор шума;
- СФ - Сетевой помехоподавляющий фильтр;
-  - Рулонные шторы blackout и решетки.

Заключение

В результате выполнения курсовой работы я спроектировал инженерно-техническую систему защиты информации для предприятия «Энигма», которая занимается разработкой специализированного программного обеспечения для ведения секретных операций и сбора разведывательной информации. Также научился выделять организационную структуру, провёл анализ рынка решений, а также разработал итоговый план предприятия.

Цель работы достигнута, все задачи выполнены

Список использованных источников

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — №3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 15.01.2022)