Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Колледж информатики и программирования

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению и оформлению курсового проекта

по профессиональному модулю ПМ.03
Защита информации техническими средствами
для студентов 4 курса
специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рассмотрен
предметной (цикловой) комиссией
обеспечение информационной безопасности
автоматизированных систем
«09» сентября 2021г.
Протокол № 2

Председатель предметной (цикловой) комиссии:
_____ /С.М. Володин/

Преподаватель _____ /С.М. Володин/

Преподаватель _____ /А.П. Филатов/

Москва 2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Курсовой проект является одной из форм учебной деятельности, которая выполняется студентом самостоятельно под руководством преподавателя. Курсовой проект представляет собой учебно-исследовательскую деятельность, требующую от студентов освоения элементов научного исследования. Выполнение курсового проекта направлено на формирование у студентов способностей:

- самостоятельно мыслить,
- анализировать и сопоставлять факты,
- обобщать и логически излагать материал.

В результате выполнения курсового проекта у студентов формируется субъективно новое знание по одной из частных проблем.

В ходе работы над курсовым проектом у студента развивается научная наблюдательность, студент учится не только находить необходимую информацию, но и корректно ее использовать в своем исследовании, грамотно демонстрировать, как и откуда были получены те или иные сведения, и каково их значение для данного исследования.

Курсовой проект способствует формированию у студентов опыта самостоятельного научного творчества, повышению уровня теоретической и профессиональной подготовки, лучшему усвоению учебного материала.

В процессе работы над проектом студент должен показать практические навыки работы с персональным компьютером, анализировать различные источники литературы, делать обоснованные выводы и предложения.

Во время курсового проектирования студенту необходимо показать умение подбирать и обоснованно использовать научную литературу, понимать логику изложения материала, уметь систематизировать данные, обрабатывать фактический материал, делать обобщения и выводы, увязывать теорию с практикой и современной действительностью.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Курсовой проект является одной из важнейших форм учебной работы и выполняется студентом в соответствие с учебным планом. Выполнение курсового проекта способствует углубленному усвоению лекционного материала и приобретению навыков в области оценки информации, создания комплексной системы защиты информации. Курсовой проект базируется на изучении законов, подзаконных актов и нормативных документов в области защиты информации, методических материалах по данной тематике, а так же лекционном материале.

Выполнение работы требует от студента не только знаний общей и специальной литературы по теме, но и умение анализировать имеющуюся информацию, принимать решения по различным вопросам, увязывать вопросы теории с практикой, делать выводы и предложения по созданию комплексной системы защиты информации. Все шаги, предпринятые студентом, все умозаключения, которые он произвёл в ходе выполнения курсового проекта должны быть им аргументированы, доказуемы и однозначно интерпретируемы.

Хотя в рамках данного методического пособия делается акцент на разработку КСЗИ для выделенных помещений, студенты не ограничены темами, предложенными в данном методическом пособии, и могут предложить свой объект защиты для исследования и разработки для него проекта комплексной системы защиты информации. Для охвата всей тематики курса в рамках данного методического пособия принято решение ограничить число студентов по темам курсового проектирования (не более одного студента на одну тему). Только если, выбранный студентами самостоятельно реальный объект защиты слишком сложен для анализа и разработки, то допускается работа над этим объектом одного-двух студентов.

Для выполнения курсового проекта студенты могут и должны пользоваться различной литературой: законами, нормативами,

руководящими документами, ГОСТами, ОСТми, периодической литературой, лекциями, специальной литературой, методическими пособиями, книгами по тематики курсовой работы и т.п., а так же руководителя курсового проектирования. На качество курсового проекта существенное влияние оказывает умелое использование практического и теоретического материалов. Подбор данных, их критическое осмысление и обработка составляют важнейший этап в подготовке и написании курсовой работы.

2. ТРЕБОВАНИЯ К СТРУКТУРЕ КУРСОВОЙ РАБОТЫ

Любая работа, которая требует разработки, начинается с Технического задания. Техническое задание (далее – ТЗ) является основным документом, определяющим требования и порядок создания (развития или модернизации - далее создания) какой либо системы, в соответствии с которым проводится разработка системы и ее приемка при вводе в действие.

Особенности учебного процесса вносят свои коррективы в создание ТЗ. В частности, является затруднительным детальное изучение разрабатываемой системы студентом до получения им ТЗ, так как ТЗ в учебном процессе, по сути, является указанием начала выполнения курсового проекта. В связи с этим, ТЗ, создаваемое в рамках данного методического пособия, не содержит в себе тех разделов, которые подразумеваются ГОСТ. Однако, для развития у студентов навыков реальной работы, разработка разделов, не вошедших в ТЗ, предусмотрена непосредственно в ходе выполнения курсового проекта.

Содержание работ по разработке и утверждению Технического задания Техническое задание (ТЗ) разрабатывается на основе задания, выданного студенту. В данном случае студент выступает в роли Исполнителя, руководитель от выпускающей ПЦК – Заказчиком ТЗ, а руководитель курсового проектирования в роли третьего лица, согласующего ТЗ в целом.

Разработанный студентом проект ТЗ согласовывается руководителем курсового проектирования и утверждается руководителем профильной ПЦК.

Все этапы курсового проектирования, начиная с разработки технического задания до защиты курсового проекта, выполняются в рамках учебных занятий по курсовому проектированию по МДК03.02 МДК.03.02 Инженерно - технические средства защиты информации. Время выполнения, оформления и защиты курсового проекта – 30 академических часов. За данный период времени студент и руководитель курсового проектирования обязаны выявить, обсудить и устранить все замечания по представленному на согласование проекту ТЗ.

3. СОДЕРЖАНИЕ ОСНОВНОЙ ЧАСТИ КУРСОВОГО ПРОЕКТА

ТЗ, разрабатываемое студентом в рамках выполнения курсового проектирования, содержит как минимум следующие разделы, которые допускается делить на подразделы:

1. Описание объекта защиты. Данный раздел содержит краткое описание объекта защиты. Все необходимые данные об объекте должны быть занесены в приложения к ТЗ.

2. Целевая установка.

Курсовая работа является завершающим этапом изучения дисциплины. Формулируемая студентом цель курсового проектирования должна быть четкой, прозрачной и достижимой. Достижение поставленной цели при выполнении курсовой работы(работы) является одним из критериев её оценки – нечеткая, неточная или заранее недостижимая цели существенно затруднит защиту курсовой работы(работы).

3. Основные разделы. Раздел содержит название основных этапов выполнения курсовой работы(работы);

− Анализ объекта защиты.

− Формирование требований к создаваемой КСЗИ.

− Разработка концепции, создаваемой КСЗИ.

4. Источники. В данном разделе перечисляются базовые нормативные и методические материалы, которыми студент будет руководствоваться в своей деятельности.

Пример оформления в соответствии с данными требованиями ТЗ представлен в Приложении Г

− Приложение А. Содержит варианты заданий на курсовое проектирование. В этом пронумерованном списке под каждым номером находится вариант задания, состоящий из цифр номера зачетной книжки. На основе этих данных студент формирует свое ТЗ.

− Приложение Б. График выполнения курсового проекта.

− Приложение В. Титульный лист курсового проекта.

В рамках данного методического пособия студенту предлагается воспользоваться приложениями для разработки курсового проекта и приложений к нему: Приложение Д

- Территориальный план местности, с расположенным на нём зданием.
- План выделенного помещения.
- Модели бизнес - процессов
- Сводные таблицы с данными о выделенном помещении.
- Графики анализа угроз

4. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

4.1. МЕТОДИКА ПРОВЕДЕНИЯ КОМПЛЕКСНОГО АНАЛИЗА ИНФОРМАЦИННОЙ БЕЗОПАСНОСТИ

Согласно вышесказанному, объектом защиты, рассматриваемому в рамках данного методики, является информация, её носители и средства обработки, в том числе и персонал. Выполнение раздела «Анализ объекта защиты» проводится в два этапа:

Этап 1 – Описание информационных ресурсов;

1.1. Определение сведений, возможно подлежащих защите

Задача данного этапа: Выявить все информационные ресурсы, которые тем или иным образом обрабатываются (могут быть обработаны) в рассматриваемом выделенном помещении.

Входные данные Материалы, представленные в ТЗ.

Способ выполнения: Выявление обрабатываемых информационных ресурсов при выполнении работ по реальным объектам заключается в обследовании средств обработки информации с целью выявления, классификации и описания обрабатываемой информации. В случае если студент выполняет курсовой проект, по варианту, предложенному в данном методическом пособии, то он должен самостоятельно, основываясь на исходных данных, разработать перечень обрабатываемой в выделенном помещении информации.

Критерии выполнения: Результатом выполнения этапа должен явиться перечень обрабатываемой в выделенном помещении информации с необходимыми комментариями и справочными сведениями. Какие именно сведения и комментарии следует приложить к перечню, какой формы следует сделать перечень – определяется студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту (работе).

Помощь

Иногда целесообразно объединить выполнение этого этапа КП с двумя следующими этапами. Для этого рекомендуется применять методики моделирования бизнес-процессов, таких как IDEF0, IDEF3, IDEF5, ARIS, UML и им подобные.

1.2. Описание защищаемой информации

Задача данного этапа на основе перечня сведений, разработанном в ходе выполнения пункта 1.1, а так же сведений, представленных в ТЗ ответить на вопросы:

− Что/Кто является источниками этой информации?

− Что/Кто является носителями этой информации?

− Где в выделенном помещении находится информация?

− Кто имеет доступ к информации?

Входные данные:

Материалы, представленные в ТЗ, перечень сведений, обрабатываемых в выделенном помещении.

Способ выполнения:

Ответ на представленные выше вопросы производится, так же, как и входе выполнения этапа 1.1 с помощью анализа средств обработки информации.

Критерии выполнения

Результатом выполнения этапа должен явиться структурированный массив информации, максимально полно отвечающий на поставленные вопросы. Полнота представления информации не должна быть использована в ущерб наглядности представления и удобства пользования собранной информацией. Выбор формы представления и информационная наполненность определяются студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту.

Иногда целесообразно объединить выполнение пункта 1.2 с пунктами 1.1, 1.3. Для этого рекомендуется применять методики моделирования бизнес-процессов, таких как IDEF0, IDEF3, IDEF5, ARIS, UML и им

подробные. Представление массива информации в виде сводной таблицы целесообразно лишь для перечня с малым количеством пунктов.

1.3. Описание информационных процессов.

На основе данных, подготовленных в ходе выполнения пунктов 1.1 и 1.2, а также сведений, представленных в ТЗ ответить на вопросы:

− В каких информационных процессах используется информация?

− Какие действия производятся над информацией?

− Какую роль играют рассматриваемые информационные процессы в функционировании организации в целом?

Входные данные

Материалы, представленные в ТЗ, данные, подготовленные в ходе выполнения пунктов 1.1 и 1.2.

Способ выполнения:

Ответ на представленные выше вопросы производится, так же, как и входе выполнения пункта 1.1 с помощью анализа средств обработки информации.

Критерии выполнения

Результатом выполнения данного пункта должен явиться структурированный массив информации, максимально полно отвечающий на поставленные вопросы. Полнота представления информации не должна быть использована в ущерб наглядности представления и удобства пользования собранной информацией. Выбор формы представления и информационная наполненность определяются студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту.

Иногда целесообразно объединить выполнение пункта 1.3 с пунктами 1.1, 1.2. Для этого рекомендуется применять методики моделирования бизнес-процессов, таких как IDEF0, IDEF3, IDEF5, ARIS, UML и им подобные.

1.4. Категорирование информации.

Задача данного пункта.

На основе данных, подготовленных в ходе выполнения пунктов 1.1 – 1.3 определить ценность рассматриваемой информации (информационных ресурсов) для организации.

Входные данные Данные, подготовленные в ходе выполнения пунктов 1.1 – 1.3.

Способ выполнения:

Первое, что должен выполнить студент, это определиться с применяемой им методикой ранжирования информации (информационных ресурсов) по степени важности для их собственника (владельца и т.д.). Второе, провести оценку ценности рассматриваемой информации (информационных ресурсов) в соответствии с выбранной методикой.

Критерии выполнения:

Результатом выполнения этапа должен явиться некий перечень информации (информационных ресурсов) с указанием их категории (ценности). Полнота представления информации не должна быть использована в ущерб наглядности представления и удобства пользования собранной информацией. Выбор формы представления и информационная наполненность определяются студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту (работе). Помощь Применение методик категорирования помогает реализовать дискретный подход к защите информации, предполагающий, что к информации определенной категории (ценности) следует предъявлять определённый набор требований. Студент не ограничен в выборе применяемой методики. При выборе методики категорирования (определения ценности) следует учитывать выполнения этапа.

Этап 2. Расчет информационных рисков.

2.1: Описание факторов, воздействующих на информацию на основе данных, подготовленных в ходе выполнения первого этапа курсового проектирования, сведений, представленных в ТЗ, и ГОСТ 51583-2000 выявить всё множество факторов, которые могут

воздействовать на информацию (информационные ресурсы) в рассматриваемом случае.

Входные данные, подготовленные в ходе выполнения этапа 1, ГОСТ 51583-2000, сведения, представленные в ТЗ. Способ выполнения: Допускается расширение (детализации) перечня факторов, представленных в ГОСТ 51583-2000.

Критерии выполнения Результатом выполнения пункта 2.1.должен явиться перечень факторов, воздействующих на информацию, обрабатываемую в рассматриваемом выделенном помещении.

Помощь В зависимости от конкретной ситуации целесообразно составлять либо общий перечень факторов, либо делать свой перечень для каждого информационного ресурса (группы информационных ресурсов).

2.2. Разработка модели злоумышленника

На основе подготовленных ранее описаний обрабатываемой в выделенном помещении информации, Понятием модели злоумышленника и РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» от 30 марта 1992 года разработать модель вероятного злоумышленника.

Входные данные Данные, подготовленные в ходе выполнения этапа 1, Понятие модели злоумышленника, РД.

Способ выполнения:

Разработка модели злоумышленника производится в соответствии с концепцией, представленной в лекционном курсе в разделе «Понятие модели злоумышленника». Студент вправе применять иную концепцию, либо модифицировать имеющуюся. Единственное требование при этом – аргументированность действий и доказуемость результатов.

Критерии выполнения Результатом выполнения этапа должна явиться максимально адекватная существующей действительности модель вероятного злоумышленника максимально.

Форма представления разработанной модели не регламентируется. Единственное требование, наглядность и достаточная полнота представляемых сведений.

Помощь Зачастую разработать полную, детализированную модель вероятного злоумышленника не представляется возможным. В таких случаях следует ограничиться сбором данных в объеме, позволяющем выполнять следующие этапы. В ситуациях, когда и такую информацию собрать не удаётся, следует вместо недостающих данных ввести предположения, а дальнейшем ссылаясь на это.

2.3. Описание уязвимостей

На основе анализа данных, представленных в ТЗ и анализа реального состояния дел выявить максимально полный перечень уязвимостей, которыми обладает выделенное помещение и средства обработки информации, находящиеся в нём.

Входные данные Данные, представленные в ТЗ, анализ выделенного помещения, справочники уязвимостей конкретных информационных систем.

Способ выполнения: На основе анализа исходных данных, реального состояния дел и справочников возможных уязвимостей, определяются уязвимости, которыми обладает выделенное помещение и средства обработки информации. В случае, когда студент выполняет курсовой проект по варианту, предложенному данным методическим пособием, и в исходных данных не содержится сведений, необходимых для более точного выявления возможных уязвимостей, он должен в ходе выполнения данного пункта самостоятельно добавить недостающие сведения.

Критерии выполнения Результатом выполнения пункта должен явиться максимально полный перечень уязвимостей рассматриваемого выделенного помещения и средств обработки информации.

Помощь При описании уязвимостей типовых систем допускает приводить ссылку на их описания. При описании уязвимостей целесообразно

отдельно проводить исследования по направлениям Организационная, Техническая и Программно-техническая защита информации.

2.4. Описание угроз

На основе сведений, полученных в ходе выполнения всех предыдущих этапов и пунктов, выявить реальные угрозы информации (информационным ресурсам), обрабатываемым в рассматриваемом выделенном помещении, описать возможные каналы реализации каждой угрозы и предположить последствия их реализации.

Входные данные Сведения, полученных в ходе выполнения этапа 1, пунктов 2.1 – 2.3 этапа 2.

Способ выполнения: При выполнении данного раздела, студенту следует проработать последовательность Информационный ресурс – Информационный процесс – Воздействующий фактор – Злоумышленник – Уязвимости.

Критерии выполнения Результатом выполнения этапа должен явиться сводный массив данных об угрозах, каналах и последствиях их реализации, оценены вероятности реализации угроз. Вероятности реализации угроз должны быть ранжированы.

Помощь При проработке цепочки Информационный ресурс – Информационный процесс – Воздействующий фактор – Злоумышленник удобно использовать древовидное представление сведений.

2.5. Расчёт информационных рисков

Задача данного этапа На основе полученных ранее сведений, для каждой из угроз для каждого информационного ресурса определить информационные риски. Проранжровать полученные значения по трехбалльной шкале (Высокие, Средние, Низкие).

Входные данные Сведения, полученных в ходе выполнения этапа 1, и пунктов 2.1 – 2.4.

Способ выполнения: Подсчет величины информационных рисков для каждой из угроз для каждого информационного ресурса приводится в соответствии с методикой, предложенной в разделе лекций «Информационные риски». Студент может предложить свой вариант методики оценки. Единственное требование – аргументированность действие и доказуемость результатов.

Критерии выполнения Результатом выполнения этапа является проранжированная оценка информационных рисков рассматриваемым информационным ресурсам.

Помощь Для оценки информационных рисков рекомендуется применять механизмы анализа иерархий.

Этап 3. Формирование требований к создаваемой КСЗИ

3.1. Общие сведения о КСЗИ

Имея после выполнения этапа «Анализ объекта защиты» максимально полную картину об объекте защиты и информационных рисках, студент имеет возможность сформулировать то, что он хочет получить от КСЗИ, т.е. сформулировать набор требований к КСЗИ. Согласно ГОСТ 34.602-89 и с учетом особенностей учебного процесса при подготовке ТЗ на любую КСЗИ должны быть сформулированы следующие наборы требований:

− требования к структуре и функционированию КСЗИ;

− требования к численности и квалификации обслуживающего персонала и пользователей КСЗИ;

− показатели надежности функционирования КСЗИ;

− показатели эффективности функционирования КСЗИ;

− требования к безопасности КСЗИ;

− требования к информационной безопасности КСЗИ (НСД, сохранность при чрезвычайных ситуациях);

− требования к защите от внешних воздействий компонент и КСЗИ в целом;

− дополнительные требования.

Как видно из представленного списка студент не ограничен в расширении, дополнении и уточнении набора требований, предъявляемых КСЗИ. В случае, когда сформулировать требование в явном виде не представляется возможным, допускается пропустить описание такого требования, однако необходимо обосновать принятие данного решения.

3.2. Формулирование требований к КСЗИ

Задача данного этапа На основе полученных ранее сведений, сформулировать набор требований к КСЗИ.

Входные данные Сведения, полученные в ходе выполнения раздела «Анализ объекта защиты»

Способ выполнения:

Формулирование требований к КСЗИ в рамках выполнения данного курсового проекта требует от студента поставить себя на место сотрудников организации, работающей в рассматриваемом выделенном помещении. Студент должен иметь представления о реальной работе организация для грамотного и полного формулирования требований.

Критерии выполнения

Результатом выполнения пункта КП является максимально полное описание каждого из требований и, в некоторых случаях, доказательства почему то или иное требование не представляется возможным сформулировать.

Помощь При выполнении данного раздела студенту рекомендуется обращаться за консультациями к людям, уже имеющих опыт работ в сфере близкой к сфере работы организации.

3.4. Разработка концепции КСЗИ

Общие сведения Концепция КСЗИ – система взглядов, выражающая определенный способ видения ("точку зрения"), понимания, трактовки КСЗИ. Концепция КСЗИ – предложение использование некоторого набора мер по защите информации, предложения по составу этих мероприятий. Разработка комплексной системы защиты информации процесс творческий и

в большей степени зависит от опыта и взглядов разработчика системы информационной безопасности, т. е. студента выполняющего работу. Как результат – множество взглядов на решение одной и той же проблемы. Основная задача данного радела – рассмотреть несколько наиболее удачных концепций КСЗИ и выбрать наиболее соответствующую разработанным в ходе выполнения предыдущего раздела требованиям к КСЗИ.

3.5. Основные принципы защиты информации

Построение системы защиты полезно проводить с принципами, на которые необходимо опираться, чтобы система защиты была отлаженной и эффективной. Под принципами защиты информации понимаются основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения ценных сведений. Наиболее распространенными принципами являются:

− Адекватность (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемой информации. Если, например, оборот компании составляет 10 тыс. рублей в месяц, вряд есть смысл развертывать систему защиты на миллион. То же самое и наоборот, если доходы компании достаточно большие, то экономия на защите информации не даст необходимого эффекта, не все каналы утечки будут перекрыты, а следовательно, злоумышленник сможет ими воспользоваться для реализации атаки;

− Системность. Важность этого принципа состоит в том, что система защиты информации должна строиться не абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств и построения системы;

− Прозрачность для сотрудников. Введение механизмов безопасности по ограничению доступа к защищаемой информации может приводить к усложнению действий сотрудников при выполнении ими своей работы. При

создании системы защиты стоит учитывать, что никакой механизм не должен требовать невыполнимых действий от сотрудников предприятия или на слишком долгое время затягивать процедуру доступа к информации;

− Равностойкость звеньев системы защиты. Звенья - это элементы защиты, преодоление любого из которых означает преодоление всей защиты. Нельзя слабость одних звеньев компенсировать усилением других. В любом случае, прочность защиты определяется прочностью самого слабого звена. И если нелояльный сотрудник готов за определенные услуги сотрудничать со злоумышленником, то вряд злоумышленник ли будет выстраивать сложную атаку для достижения цели.

− Непрерывность. Почти тоже самое, что и равностойкость, только во временной области. Защищаемую информацию и ее носителей необходимо защищать в любой момент времени. Нельзя, например, решить по пятницам делать резервное копирование информации, а в последнюю пятницу месяца устроить «санитарный день». Может случиться, что именно в тот момент, когда меры по защите информации будут ослаблены, злоумышленник может реализовать угрозу. Временный провал в защите информации, делает ее бессмысленной и неэффективной;

− Многоуровневость. Защита должна строиться в несколько уровней, которые должен преодолевать как злоумышленник, так и сотрудники предприятия? Потому что всегда существует вероятность того, что какой-то уровень может быть преодолен либо в силу непредвиденных случайностей, либо с ненулевой вероятностью. И, если один уровень гарантирует защиту в 90%, то три уровня (ни в коем случае не повторяющих друг друга) – 99,9%. Принципы реализации КСЗИ можно разделить на три группы: − правовые; − организационные;

− принципы, используемые при защите информации от технических средств разведки и в средствах вычислительной техники. Основными правовыми принципами защиты информации являются следующие:

− принцип законности – выражается прежде всего в том, что необходимо нормативно-правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации; определено, что является секретными и конфиденциальными сведениями; установлена уголовная, административная, материальная, моральная ответственность за незаконное покушение на защищаемую информацию и последствия для собственника;

− принцип приоритета международного права над внутригосударственным.

− принцип собственности и экономической целесообразности. Этот принцип дает право принимать меры к защите информации, а также оценивать ее потребительские свойства. Организационные принципы защиты информации заключаются в следующем:

− научный подход к организации защиты информации, в основе которого лежит системный подход. Системный подход к организации защиты информации позволяет создать органически взаимосвязанную совокупность сил, средств и специальных методов по оптимальному ограничению сферы обращения засекреченной информации, предупреждение ее утечки;

− максимальное ограничение числа лиц, допускаемых к защищаемой информации, т. к. сохранность засекреченной информации находиться в зависимости от количества лиц, допущенных к обращению с нею;

− дробление технологической цепочки производства на отдельные операции, знание одной из которых не дает возможность восстановить всю технологию;

− персональная ответственность за сохранность доверенных секретов;

− единство в решении производственных, коммерческих, финансовых, кадровых и режимных вопросов;

− непрерывность защиты информации предполагает, что защита конфиденциальной информации должна начинаться с момента ее появления на всех этапах ее обработки, передачи, использования и хранения, вплоть до этапа ее уничтожения. Принципы защиты информации, используемые при организации противодействия техническим средствам разведки (ТСР):

− активность защиты информации - выражается в целенаправленном навязывании технической разведке ложного представления об объекте его разведывательных устремлений, в соответствии с замыслом защиты;

− убедительность защиты информации - состоит в оправданности замысла защиты условиям обстановки в соответствии с характером защищаемого объекта или свойствам окружающей среды, в применении технических решений защиты, соответствующих климатическим, сезонным и другим условиям;

− непрерывность защиты информации предполагает организацию защиты объекта на всех стадиях организации его жизненного цикла;

− разнообразие защиты информации – предусматривает исключение шаблона, повторяемости в выборе объекта прикрытия и путей реализации смысла защиты, в том числе с применением типовых решений. Из-за повсеместного использования компьютеров на предприятиях стоит привести принципы защиты информации, используемые в системах вычислительной техники:

− введение избыточности элементов системы;

− резервирование элементов;

− защитные преобразования данных;

− контроль состояния элементов системы, их работоспособности и правильности функционирования.

3.6. Методы защиты информации

При реализации системы защиты необходимо определиться с методами защиты. Невозможно найти один способ (метод) защиты информации от всех угроз. В зависимости от ситуации (угрозы) действия по защите будут

разными, следовательно, и методы должны быть тоже разными. Метод – в самом общем значении это способ достижения цели, определенным образом упорядоченная деятельность. В области защиты информации разработано достаточное количество методов, среди которых можно выбрать наиболее подходящий для конкретной ситуации при разработке системы защиты.

Основные методы, используемые в защите информации:

− скрытие;

− ранжирование;

− дезинформация;

− дробление;

− страхование;

− морально-нравственные;

− учет;

− кодирование;

− шифрование.

Скрытие – как метод защиты информации является в основе своей реализации на практике одного из основных организационных принципов защиты информации - максимального ограничения числа лиц, допускаемых к сведениям. Реализация этого метода достигается обычно путем:

− засекречивание информации, то есть отнесение ее к секретной или конфиденциальной информации различной степени секретности и ограничение в связи с этим доступа к этой информации в зависимости от ее важности для собственника, что проявляется в поставляемом на носителе грифе секретности;

− устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

Скрытие – один из наиболее общих и широко применяемых методов защиты информации.

Ранжирование как метод защиты включает, во-первых, деление засекречиваемой информации по степени секретности, и, во-вторых,

регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации. Ранжирование как метод защиты информации является частным случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

Дезинформация – один из методов защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-либо объектов и изделий, действительного состояния положения дел на предприятии и т.д. Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты, и др. Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации не позволяет восстановить всю картину, всю технологию в целом.

Страхование – сущность данного метода сводится к тому, чтобы защитить права и интересы собственника информации или средства информации как от случайных угроз (кражи, стихийные бедствия), так и от преднамеренных угроз безопасности информации, а именно: защита информации о утечки, хищения, модификации (подделки), разрушения и др. При страховании информации должно быть проведено аудиторское обследование и дано заключение о сведениях, которые предприятие будет защищать как коммерческую тайну и надежности средств защиты. Морально-нравственные методы защиты информации можно отнести к

группе тех методов, которые, играют очень важную роль в защите информации. Поскольку именно человек, сотрудник предприятия, допущенный к защищаемым сведениям и накапливающий в своей памяти колоссальные объемы информации, в том числе секретной или конфиденциальной, нередко становится источником утечки этой информации или по его вине злоумышленник получает возможность несанкционированного доступа к носителям защищаемой информации. Данные методы защиты информации предполагают, прежде всего, воспитание сотрудника, допущенного к защищаемым сведениям, то есть проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение сотрудника, осведомленного в сведениях, составляющих тайну, правилам методам защиты информации, привитие ему навыков работы с носителями секретной или конфиденциальной информации.

Учет также один из важнейших методов защиты информации, обеспечивающий возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также о всех пользователях этой информации. Без учета решать проблемы было бы невозможно, особенно когда количество носителей превысит какой-то минимальный объем.

3.7. Меры защиты информации

При разработке концепции КСЗИ в условиях выбранной политики управления информационными рисками и применяемыми методами защиты информации предполагается формирование нескольких наборов мер по защите информации с примерной оценкой их состава. Разработанные варианты концепции затем оцениваются экспертами по критериям эффективности и стоимости. На основании оценки принимается решение выбрать ту или иную концепцию. Существует множество классификаций применяемых мер защиты. Так, стандарт ГОСТ 17799-2005 определяет 11

групп мер по защите информации, классификация по признаку «целевой канал утечки информации» приводит к появлению двух групп методов: «меры, направленные на противодействие агентурному каналу утечки информации» и «меры, направленные на противодействие техническим каналам утечки информации».

Этап 4. Разработка варианта концепции КСЗИ

Задача данного этапа На основе анализа данных, подготовленных на предыдущих этапах разработать вариант концепции КСЗИ.

Входные данные - данные, подготовленные на трех предыдущих этапах. Способ выполнения: На основе сведений об информационных рисках для каждого из информационных ресурсов, обрабатываемых в выделенном помещении, выбирают конкретный метод управления рисками для каждого из ресурса. Для каждого информационного ресурса выбирается предпочтительный метод защиты и делается предположение о возможном наборе мер для поддержки реализации метода. Совокупность выбранных методов управления рисками, методов защиты информации и предполагаемых мер защиты составляет концепцию КСЗИ.

Критерии выполнения Результатом выполнения этапа должен явиться концепция КСЗИ.

Помощь Выбор определённого метода управления рисками и метода защиты может быть упрощен, если поставить в соответствие конкретному значению набора критериев КЦД конкретный набор методов управления рисками и защиты.

4.1. Разработка проектного решение по КСЗИ

Общие сведения Проектное решение КСЗИ является непосредственной реализацией выбранной концепции КСЗИ. Разработка проекта КСЗИ ведется студентом на основании знаний, полученных в результате изучения данного и остальных учебных курсов. При необходимости студент может привлекать отечественные и зарубежные нормативные документы и методики, каталоги средств защиты информации и т.п. сведения.

Задача данного этапа На основе всех ранее собранных данных разрабатывается проектное решение по КСЗИ.

Входные данные, подготовленные на предыдущих этапах, отечественные и зарубежные нормативные документы, методики, каталоги средств защиты и т.п. сведения.

Способ выполнения: На основе разработанной концепции КСЗИ производится разработка общих решений по КСЗИ в целом и ее частям, функционально структуре КСЗИ, по функциям персонала и организационной структуре, по структуре технических средств и по программному обеспечению.

Критерии выполнения Разработанный проект КСЗИ должен максимально полно отвечать требованиям, сформулированным в ходе выполнения этапа №3, а так же целям выполнения данного курсового проекта.

Помощь Разработке проекта КСЗИ может значительно помочь анализ уже выполненных проектов КСЗИ по схожим проектам.

Выводы по курсовому проекту.

Задача данного этапа Подвести итоги выполненной работы. Оценить достижение целей и задач, поставленных в ТЗ. Оценить текущую защищенность объектов защиты.

Входные данные Данные, подготовленные на всех этапах КП.

Способ выполнения: Выводы являются кратким изложением работы, проделанной студентом в ходе выполнения курсовой работы(работы), отражением основных полученных результатов, описанием того, что было выполнения для достижения цели курсовой работы, а что не удалось. Критерии выполнения

В заключительной части курсового проекта должны присутствовать выводы как по отдельным частям работы, так и по всей работе в целом.

Помощь Подведение выводов по выполненному курсовому проекту значительно упростится, если в конце выполнения каждого из этапов работы

студент будет формулировать частные выводы, наиболее важные из которых затем вынесет в заключительную часть проекта.

5. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ПОЯСНИТЕЛЬНОЙ ЗАПИСКИ КУРСОВОГО ПРОЕКТА

Пояснительная записка курсового проекта должна быть оформлена в соответствии с требованиями ГОСТ 7.32. – 2001 «Система стандартов по информации, библиотечному и издательскому делу «Отчет о научно-исследовательской работе. Структура и правила оформления», ГОСТ 7.1. – 2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления», ГОСТ 7.82. – 2001 «Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления», Единой системы программной документации (ЕСПД).

5.1 Общие требования к оформлению

Страницы текста пояснительной записки, а также иллюстрации и таблицы должны соответствовать формату А4 и быть выполнены с использованием компьютера и принтера на одной стороне листа белой бумаги формата А4 через полтора интервала.

Цвет шрифта должен быть черным. Высота и стиль букв, цифр и других знаков должны соответствовать кеглю 14, шрифту Times New Roman.

Текст пояснительной записки должен быть выровнен по ширине, начертание обычное.

Текст пояснительной записки следует печатать, соблюдая следующие размеры полей:

- правое–10 мм;
- верхнее и нижнее – 20 мм;
- левое– 30 мм.

Абзацный отступ (красная строка) должен составлять12,5 мм.

Разрешается использовать компьютерные возможности акцентирования внимания на определенных терминах, формулах, теоремах, применяя шрифты разной гарнитуры.

Фамилии, названия учреждений, организаций, фирм, название изделий и другие имена собственные в пояснительной записке приводят на языке оригинала. Допускается транслитерировать имена собственные и приводить названия организаций в переводе на язык пояснительной записки с добавлением (при первом упоминании) оригинального названия.

Наименования структурных элементов пояснительной записки «СОДЕРЖАНИЕ», «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ», «ПРИЛОЖЕНИЕ» служат заголовками структурных элементов. Заголовки структурных элементов следует располагать в середине строки без точки в конце и печатать прописными буквами, не подчеркивая.

Каждый структурный элемент пояснительной записки, а также каждый новый раздел следует начинать с нового листа (страницы).

Основную часть пояснительной записки следует делить на разделы, подразделы и пункты. Пункты, при необходимости, могут делиться на подпункты. При делении текста на пункты и подпункты необходимо, чтобы каждый пункт содержал законченную информацию.

Разделы, подразделы должны иметь заголовки. Пункты, как правило, заголовков не имеют. Заголовки должны четко и кратко отражать содержание разделов, подразделов.

Заголовки разделов, подразделов и пунктов следует печатать с абзацного отступа с прописной буквы без точки в конце, не подчеркивая. Если заголовок состоит из двух предложений, их разделяют точкой.

Заголовок раздела отделяется от заголовка подраздела одной пустой строкой. Текст подраздела отделяется от заголовка подраздела также одной строкой.

Страницы пояснительной записки следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту пояснительной записки. Номер страницы проставляют в центре нижней части листа без точки.

Титульный лист включают в общую нумерацию страниц пояснительной записки. Номер страницы на титульном листе не проставляют.

Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц.

Разделы пояснительной записки должны иметь порядковые номера в пределах всей пояснительной записки, обозначенные арабскими цифрами без точки и записанные с абзацного отступа.

Подразделы должны иметь нумерацию в пределах каждого раздела. Номер подраздела состоит из номеров раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится, например:

3 Методы испытаний

Если раздел состоит из одного подраздела, то подраздел не нумеруется. Если подраздел состоит из одного пункта, то пункт не нумеруется.

Если текст пояснительной записки подразделяется только на пункты, то они нумеруются порядковыми номерами в пределах всей записки. Пункты, при необходимости, могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта, например 4.2.1.1, 4.2.1.2, 4.2.1.3 и т.д.

Внутри пунктов или подпунктов могут быть приведены перечисления. Перед каждым элементом перечисления следует ставить дефис. При необходимости ссылки в тексте пояснительной записки на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв ё, з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа.

5.2. **Требования к оформлению иллюстраций**

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в пояснительной записке непосредственно после текста, в котором они упоминаются впервые, или на следующей странице, с выравниванием по центру.

Иллюстрации, за исключением иллюстрации приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Если рисунок один, то он обозначается «Рисунок 1». Слово «Рисунок» и его наименование располагают посередине строки.

Допускается нумеровать иллюстрации в пределах раздела. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой. Например, Рисунок 1.1.

Допускается использование цветных иллюстраций. На все иллюстрации должны быть даны ссылки в тексте пояснительной записки. При ссылках на иллюстрации следует писать «...в соответствии с рисунком 2» при сквозной нумерации и «...в соответствии с рисунком 1.2» при нумерации в пределах раздела.

Иллюстрации, при необходимости, могут иметь наименование и пояснительные данные (подрисуночный текст). Слово «Рисунок» и наименование рисунка при этом помещают под рисунком по центру, например:

Рисунок 1 – Детали прибора

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например, Рисунок А.3.

5.3. **Требования к оформлению таблиц**

Таблицы применяют для лучшей наглядности и удобства сравнения показателей. Наименование таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Наименование таблицы следует

помещать над таблицей слева, без абзацного отступа в одну строку с ее номером через тире.

Таблицу следует располагать в пояснительной записке непосредственно после текста, в котором она упоминается впервые, или на следующей странице.

Таблицы следует располагать по ширине документа. Заголовки столбцов должны быть центрированы, а остальной текст должен быть выровнен по левому краю. Шрифт в таблице должен быть таким же, как и во всей пояснительной записке, однако размер шрифта может быть при необходимости уменьшен до кегля 12.

На все таблицы должны быть ссылки в тексте пояснительной записки. При ссылке следует писать слово «таблица» с указанием ее номера, например:

«В таблице 1 представлены специальные символы» или «Для явного преобразования типов существуют функции, которые приведены в таблице 2.»

Если две и более таблиц располагаются последовательно, то они разделяются одной пустой строкой.

Не должно быть пустых строк между названием таблицы и самой таблицей, а также между таблицей и последующим текстом.

Таблицу с большим числом строк допускается переносить на другой лист (страницу). При переносе части таблицы на другой лист (страницу) слово «Таблица», ее номер и наименование указывают один раз слева над первой частью таблицы, а над другими частями также слева пишут слова «Продолжение таблицы» и указывают номер таблицы.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Допускается нумеровать таблицы в пределах раздела. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения.

5.4. Требования к оформлению ссылок и списка использованных источников

Ссылки на использованные источники в тексте пояснительной записки следует указывать порядковым номером библиографического описания источника в списке использованных источников. Порядковые номера ссылок указываются арабскими цифрами и заключаются в квадратные скобки, например [5].

Список использованных источников оформляется согласно ГОСТ 7.1. – 2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления» и ГОСТ 7.82 – 2001 «Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления».

Пример оформления списка использованных источников приведен в Приложении Е.

5.5. Требования к оформлению приложений

Приложения оформляют как продолжение основного документа на последующих его листах.

В тексте пояснительной записки на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте пояснительной записки.

Каждое приложение следует начинать с новой страницы с указанием наверху посередине страницы слова «Приложение», его обозначения.

Приложение должно иметь заголовок, который записывают посередине страницы с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ъ, Ы, Ь. После слова «Приложение» следует буква, обозначающая его последовательность. Допускается обозначение приложений буквами латинского алфавита, за исключением букв I и O.В случае полного использования букв русского и латинского алфавитов допускается обозначать приложения арабскими цифрами.

Если в пояснительной записке одно приложение, оно обозначается «Приложение А».

Текст каждого приложения, при необходимости, может быть разделен на разделы, подразделы, пункты, подпункты, которые нумеруют в пределах каждого приложения. Перед номером ставится обозначение текущего приложения.

Приложения должны иметь общую с остальной частью пояснительной записки сквозную нумерацию страниц.

6. ПОРЯДОК ЗАЩИТЫ КУРСОВОГО ПРОЕКТА

После завершения работы над курсового проекта студент представляет проект руководителю для написания отзыва. В отзыве делается вывод о готовности студента к защите курсового проекта. Критериями оценки курсового проекта являются следующие:

- степень разработки темы;
- полнота охвата научной литературы;
- творческий подход к процессу курсового проектирования;
- правильность и научная обоснованность выводов;
- аккуратное и правильное оформление курсового проекта.

Отзыв руководителя на курсовой проект включает:

- заключение о соответствии курсового проекта заявленной теме;

- оценку качества выполнения курсового проекта;

- оценку полноты разработки поставленных вопросов, теоретической и практической значимости курсового проекта.

К защите курсовой проект представляется в сброшюрованном виде. Последовательность брошюровки материала: титульный лист, техническое задание, содержание, введение, основная часть, заключение, список использованных источников, приложения.

Защита курсового проекта проводится в форме выступления студента с подготовленным докладом, в котором он освещает рассмотренные им вопросы, основные теоретические сведения по теме проекта. Продолжительность доклада – 5-7 минут.

Доклад студента сопровождается презентацией, в которой необходимо отразить:

- полное наименование учебного заведения;
- тему курсового проекта;
- Ф.И.О. исполнителя и руководителя;
- год выполнения курсового проекта;
- цели и задачи курсового проекта;
- Определение сведений, возможно подлежащих защите;
- Описание защищаемой информации;
- Описание информационных процессов;
- Категорирование информации;
- Описание факторов, воздействующих на информацию4
- Разработка модели злоумышленника;
- Описание уязвимостей;
- Описание угроз;
- Расчет информационных рисков;

Заключительным слайдом презентации должен быть слайд, содержащий текст «Спасибо за внимание!».

Содержимое слайдов презентации включается в текст пояснительной записки в виде приложения.

В Приложении Ж приведен пример оформления презентации в тексте пояснительной записки.

На защите обязательно присутствуют все студенты группы, в которой проходит защита, другие студенты – по желанию. Все участники имеют право задавать вопросы по содержанию работы. Ответы на вопросы должны быть четкими и уверенными.

Курсовой проект оценивается по четырехбалльной системе. Студенты, не сдавшие в установленный срок курсовые проекты или получившие на защите неудовлетворительные оценки, не допускаются к промежуточной аттестации. Студентам, получившим неудовлетворительную оценку по курсовому проекту, предоставляется право выбора новой темы курсовой работы или, по решению преподавателя, доработка прежней темы, а также определяется новый срок для выполнения курсового проекта.

7. СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ ДЛЯ ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА

Стандарты

1. ГОСТ 7.1. – 2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления. – М.: ИПК Издательство стандартов, 2004. – 169 с.
2. ГОСТ 7.32 – 2001. Система стандартов по информацию, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления. – М.: ИПК Издательство стандартов, 2001. – 21 с.
3. ГОСТ 7.82 – 2001. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления. – М.: ИПК Издательство стандартов, 2001. –21 с.
4. Единая система программной документации. – М.: Стандартинформ, 2005. –128 с.

ПРИЛОЖЕНИЕ А

Примерные темы курсовых проектов

Последняя цифра зачетки	**Тема курсовой работы**
0	Разработка комплексной системы защиты информации складского комплекса на примере «XXXX»
1	Разработка комплексной системы защиты информации контроля территории детского сада на примере «XXXX»
2	Разработка системы защиты предприятия банковского сектора на примере «XXXX»
3	Разработка системы безопасности супермаркета на примере «XXXX»
4	Разработка комплексной системы защиты информации системы защиты спортивного – развлекательного комплекса на примере «XXXX»
5	Разработка комплексной системы защиты информации системы образовательного учреждения на примере «XXXX»
6	Разработка комплексной системы защиты информации на примере лаборатории «XXXX» Колледжа информатики и программирования
7	Разработка системы защиты серверного помещения на примере «XXXX»
8	Разработка комплексной системы защиты информации системы офисного помещения коммерческого предприятия на примере «XXXX»
9	Разработка комплексной системы защиты информации предприятия on – line торговли на примере «XXXX»

Вместо «XXXX» студент вставляет название компании на примере которой будет делать разработку проекта

Пример полной темы*:* Разработка комплексной системы защиты информации на примере лаборатории «Электроники и схемотехники» Колледжа информатики и программирования

ПРИЛОЖЕНИЕ Б

Федеральное государственное образовательное бюджетное учреждение высшего образования

«Финансовый университет при Правительстве Российской Федерации»

КОЛЛЕДЖ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УТВЕРЖДАЮ

ПМ.03 Защита информации техническими средствами

Председатель предметно - цикловой комиссии

Группа:

Обеспечение информационной безопасности АС

/ / С.М. Володин

____. ____.2021г

ПРОЕКТ КУРСОВОЙ

На тему:

_____

_____

_____

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Руководитель курсового проекта

/ / А.П. Филатов

Исполнитель курсового проекта

/ /

_____

Оценка за проект:_____

____.____.2021г

2021

ПРИЛОЖЕНИЕ В
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА

Ф.И.О. студента	Дата	Результат в %		Подпись студента	Подпись руково-дителя
		план	факт		
Иванов И.И.					

ПРИЛОЖЕНИЕ Г

Федеральное государственное образовательное бюджетное
учреждение высшего образования
Финансовый университет при Правительстве Российской Федерации

КОЛЛЕДЖ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УТВЕРЖДАЮ
Председатель предметно-цикловой комиссии
Обеспечение информационной безопасности АС

_____ФИО
«___»_____ 2021 г.

ЗАДАНИЕ НА ВЫПОЛНЕНИЕ
КУРСОВОЙ РАБОТЫ (КУРСОВОГО ПРОЕКТА)

по дисциплине (профессиональному модулю): _____

на тему: _____

Объект исследования _____
Обучающийся _____

Целевая установка: _____

Научный руководитель_____
(ученая степень, звание, Ф.И.О.)

Основные вопросы, подлежащие разработке:
1.
2.
3.
4.
5.
6.

Источники:
1.
2.
3.
4.
5.
6.

Приложения:
1.
2.

Дата выдачи задания	«___» _____ 2021
Руководитель КП _____	
Задание принял к исполнению	«___» _____ 2021
Обучающийся	

ПРИЛОЖЕНИЕ Д
ОФОРМЛЕНИЕ КУРСОВОГО ПРОЕКТА

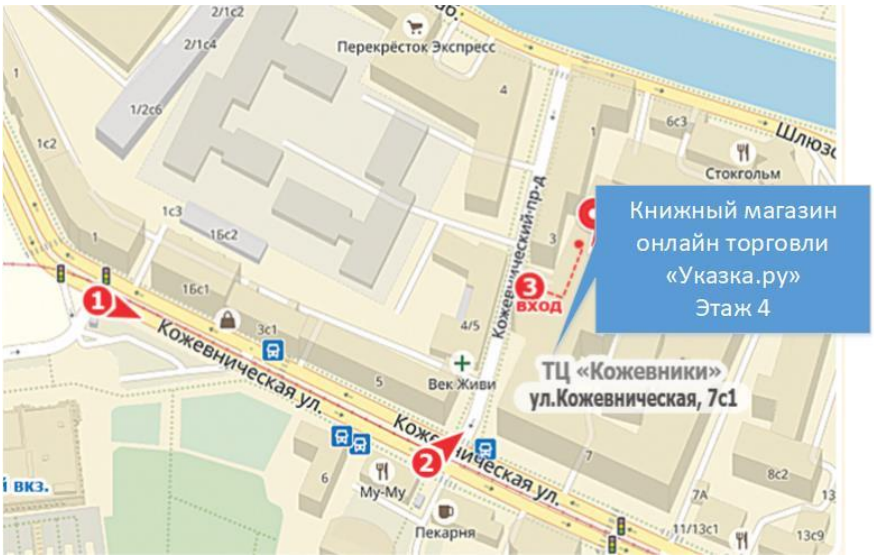

Рисунок – Схема территории

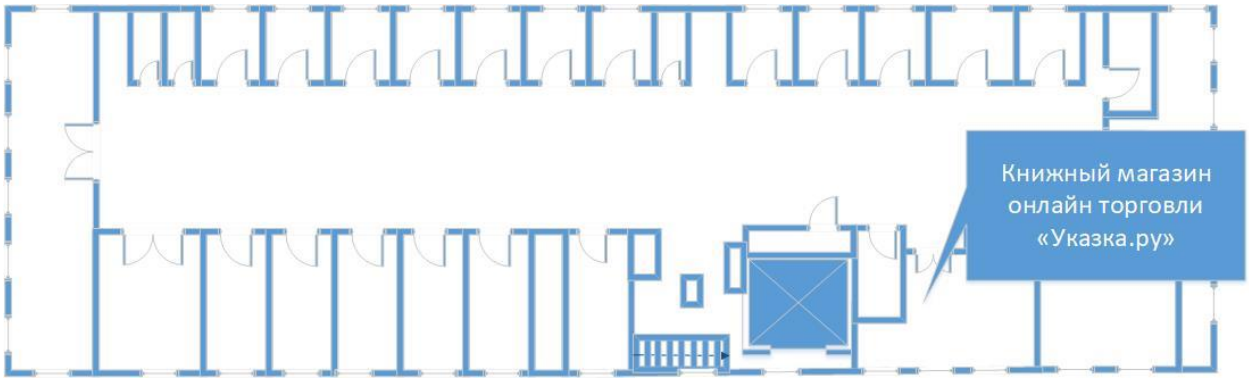

Рисунок – План помещений 4 этажа ТЦ

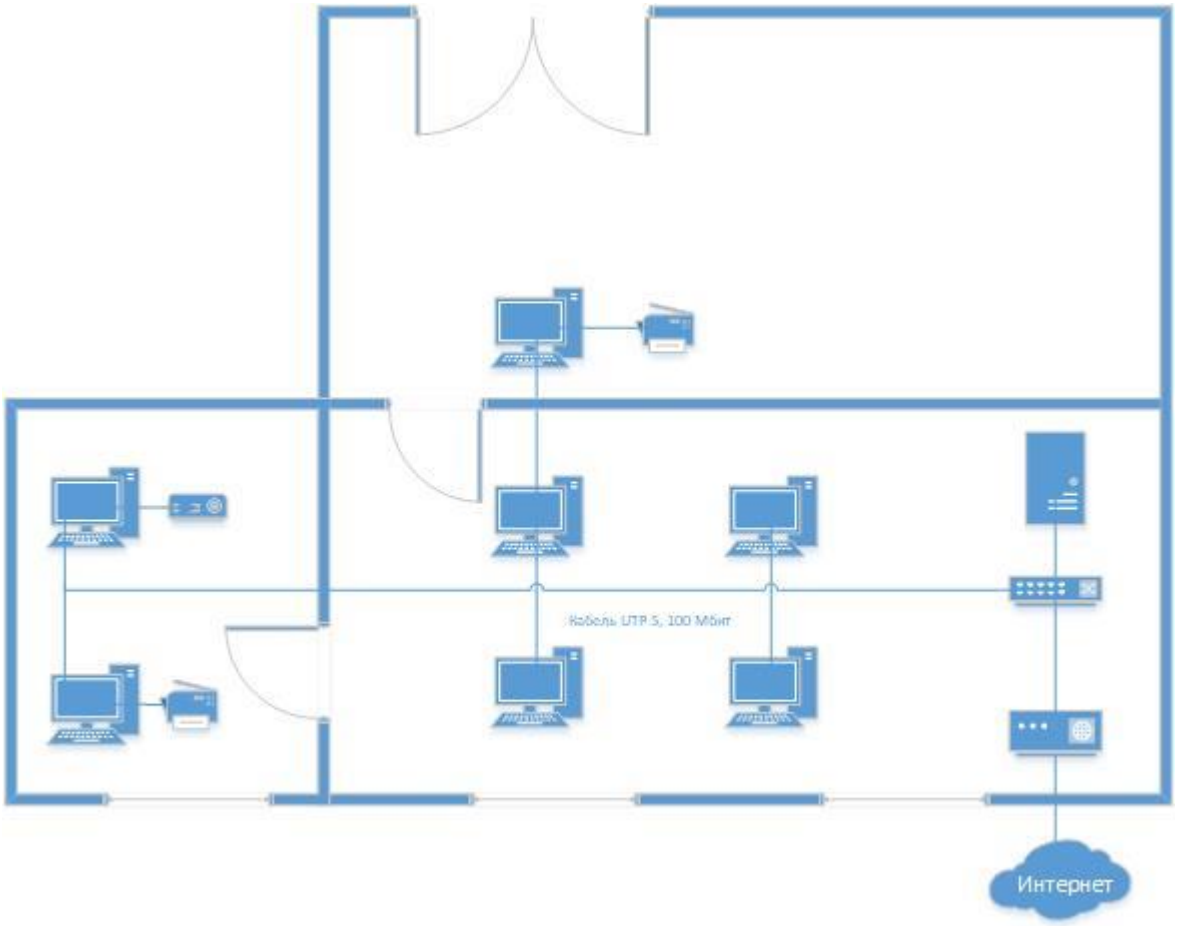

Рисунок – Схема сети ЛВС

Рисунок – Контекстная диаграмма книжный магазин онлайн торговли «Указка.ру»

Таблица. Перечень угроз

Наименование угрозы	Характеристика
Утечка данных	Действия отдельных лиц, которым удалось заполучить легитимные права доступа у информации, что привело к нарушению ее конфиденциальности. Такие действия можно разделить на две группы: преднамеренные, которые включают в себя саботаж и промышленный шпионаж, а также случайные – такие, как халатность и незнание.
Межсайтовое кодирование (XSS –атаки)	XSS (межсайтовый скриптинг) – одна из разновидностей атак на веб-системы, которая подразумевает внедрение вредоносного кода на определенную страницу сайта и взаимодействие этого кода с удаленным сервером злоумышленников при открытии страницы пользователем.
SQL — инъекции	Внедрение SQL-кода или SQL-инъекции — один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода. Внедрение SQL, в зависимости от типа используемой СУБД и условий внедрения, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.
Вредоносное программное обеспечение	Вредоносная программа – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда владельцу информации (или владельцу ЭВМ) путем копирования, искажения, удаления или подмены
Подделка межсайтовых запросов (CSRF)	CSRF («межсайтовая подделка запроса») — вид атак на посетителей веб-сайтов, использующий недостатки

	протокола HTTP.
Угроза сбоев в функционировании услуг Интернет провайдера	Сбои в функционировании услуг Интернет-провайдера в связи какими-либо обстоятельствами (техническая поломка, перегруз сети, природные аномалии и др.)
Ошибки операторов	Любое конкретное действие человека в процессе его деятельности, которое выходит за некоторые допустимые границы, т.е. превышает допуск, границы которого определены режимами работы системы.
Фишинговые атаки	Фишинг – (от англ. fishing рыбная ловля, выуживание) – вид интернет мошенничества с использованием социальной инженерии для получения доступа к конфиденциальной информации пользователей – логинам и паролям.
Атаки типа «отказ в обслуживании» (DDoS-атаки)	DDoS («отказ в обслуживании») — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён

Таблица. Неформальная модель нарушителя

Наименование	**Тип нарушителя**	**Мотивы нарушителя**	**Описание возможностей (Угроз)**
Сотрудник организации	Внутренний	- Случайные - Преднамеренные (продать информацию, промышленный шпионаж)	- Утечка данных пользователей - Заражение с помощью вредоносного ПО - Ошибки ПО
Администратор ИБ	Внутренний	- Случайные - Преднамеренные (с целью помочь конкурентам)	- Утечка данных пользователей - Заражение с помощью вредоносного ПО
Обслуживающий персонал	Внутренний	- Случайные - Преднамеренные (продать информацию, промышленный шпионаж)	- Утечка данных пользователей - Заражение с помощью вредоносного ПО - Ошибки ПО
Конкуренты	Внешний	- Преднамеренные (причинить ущерб своим конкурентам)	- Межсайтовое кодирование (XSS –атаки) - Заражение с помощью

			вредоносного ПО
Уволенные сотрудники	Внешний	- Преднамеренные (хулиганство, продажа информации)	- Утечка данных пользователей - Заражение с помощью вредоносного ПО
Хакеры	Внешний	- Преднамеренные (хулиганство, продажа информации)	- SQL-инъекция - DDOS атаки -Заражение программного кода - Подделка межсайтовых запросов(CSRF)

Таблица. Определение вероятности возникновения угроз

Ценность Актива	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8
Обозначение: Н — низкий, С — средний, В — высокий.									

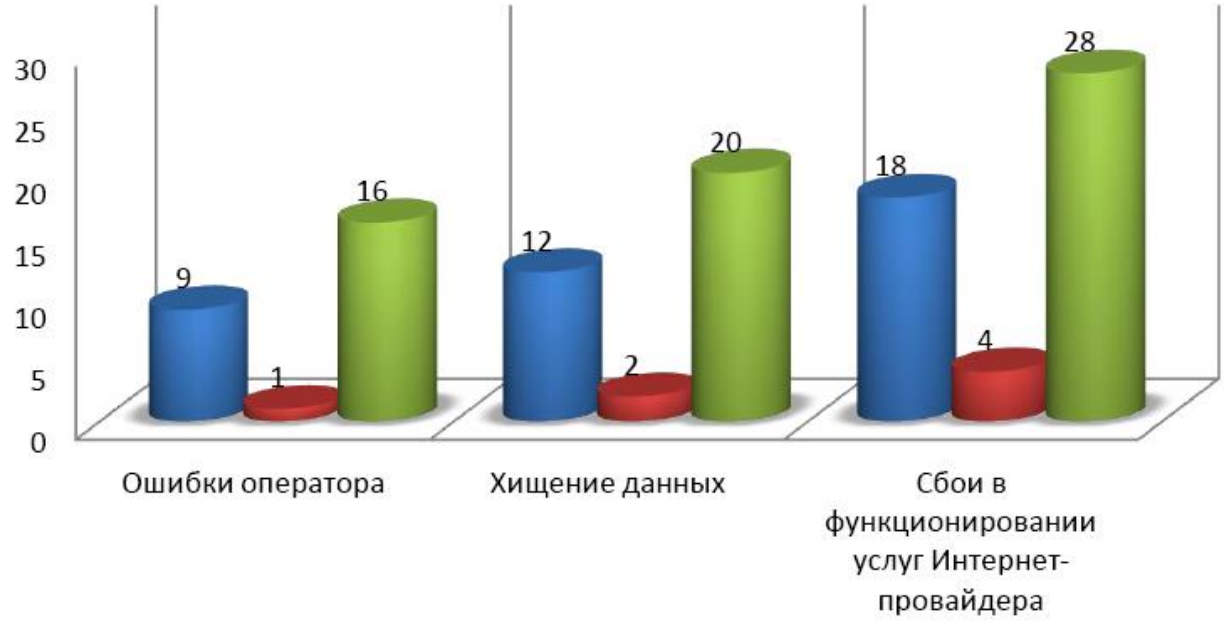

Рисунок - Риски возникновения угроз для различных активов