УТВЕРЖДАЮ
Директор ЧПОУ «КСТМ»

А.А.Батрак
« 10 » января 2023 г.

Методические рекомендации по подготовке дипломной работы для обучающихся специальности 09.02.07 Информационные системы и программирование

Москва, 2023

Методические рекомендации разработаны на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.07 Информационные системы и программирование

Организация разработчик: Частное профессиональное образовательное учреждение колледж управления и производства

Рассмотрены и одобрены:

ПЦК Социально-экономического профиля и ПЦК Технологического профиля
Протокол № 4 от «10» января 2023 г

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

Методические рекомендации по подготовке дипломной работы по специальности 09.02.07 Информационные системы и программирование составлены в соответствии с требованиями ФГОС СПО в части подготовки дипломной работы.

Дипломная работа (далее, ДР) по специальности 09.02.07 Информационные системы и программирование представляет собой исследование одной из актуальных тем в рамках содержания одного или нескольких профессиональных модулей, должна способствовать продолжению формирования профессиональных и общих компетенций, и направлена на демонстрацию сформированности компетенций, умений, знаний в рамках основных видов профессиональной деятельности, среди которых важнейшее значение имеют умения:

Анализировать проектную и техническую документацию.

Использовать специализированные графические средства построения и анализа архитектуры программных продуктов.

Организовывать заданную интеграцию модулей в программные средства на базе имеющейся архитектуры и автоматизации бизнес-процессов.

Определять источники и приемники данных.

Проводить сравнительный анализ. Выполнять отладку, используя методы и инструменты условной компиляции (классы Debug и Trace).

Оценивать размер минимального набора тестов.

Применять стандартные метрики по прогнозированию затрат, сроков и качества.

Определять метрики программного кода специализированными средствами.

Осуществлять постановку задачи по обработке информации.

Выполнять анализ предметной области.

Использовать алгоритмы обработки информации для различных приложений.

Работать с инструментальными средствами обработки информации.

Поддерживать документацию в актуальном состоянии.

Формировать предложения о расширении функциональности информационной системы.

Добавлять, обновлять и удалять данные.

Выполнять запросы на выборку и обработку данных на языке SQL.

ДР должна:

- носить творческий характер с использованием актуальных статистических данных и действующих нормативных правовых актов;
- отвечать требованиям логичного и четкого изложения материала, доказательности и достоверности фактов;
- отражать умение обучающегося пользоваться рациональными приемами поиска, отбора, обработки и систематизации информации, способности работать с нормативно-правовыми актами;
- быть правильно оформлена (четкая структура, завершенность, правильное оформление библиографических ссылок, списка литературы и нормативных правовых актов, аккуратность исполнения).

Дипломная работа может быть логическим продолжением курсовой работы, идеи и выводы которой реализуются на более высоком теоретическом и практическом уровне. *Курсовая работа может быть использована в качестве раздела дипломной работы*.

Данные методические рекомендации помогут обучающемуся избежать характерных ошибок в процессе написания ДР. Если при выполнении работы возникают не учтенные в рекомендациях нюансы, они должны решаться обучающимся и руководителем ДР в индивидуальном порядке.

2.ПОРЯДОК ВЫПОЛНЕНИЯ ДИПЛОМНОЙ РАБОТЫ

Дипломная работа выполняется на заключительном этапе обучения в виде дипломной работы. Это самостоятельное исследование по одной из актуальных тем сферы эксплуатации и обслуживания электрического и электромеханического оборудования.

Весь период подготовки и оформления ДР делится на этапы:

1. Получение задания на выполнение дипломной работы с указанием календарного графика работы над ДР.

2. Составление и согласование рабочего плана к выполнению ДР.

3. Поиск и изучение источников литературы, а также выполнение исследований по теме.

4. Написание разделов дипломной работы.

5. Оформление дополнительных материалов по ДР.

6. Подготовка презентационного материала.

7. Подготовка к защите ДР.

8. Защита ДР.

Последовательное описание основных этапов выполнения ДР указано в «Общих методических рекомендациях по выполнению дипломной работы (проекта) по специальностям среднего профессионального образования» https://cmp2014.ru/wp-content/uploads/2021/10/Obshhie-metodicheskie-ukazaniya-po-VKR-SPO-PPSSZ.pdf.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДР

3.1. Структура дипломной работы (проекта):

- титульный лист;
- задание;
- содержание;
- введение;
- глава 1 Теоретическая часть (10-20 с.);
- глава 2 Экономическая часть (10-15 с.);
- заключение (3-5 с.)
- список использованных источников;
- приложения.

Образцы написания введения, заключения и главы 1 Теоретическая часть - размещены в Приложениях № 1, № 2, № 3 настоящих методических рекомендаций.

Последовательное описание структуры ДР и макеты оформления: календарного плана выполнения дипломной работы (проекта), задания на дипломную работу (проект), отзыва на дипломную работу (проект), рецензии указаны в «Общих методических рекомендациях по выполнению дипломной работы (проекта) по специальностям среднего профессионального

образования» https://cmp2014.ru/wp-content/uploads/2021/10/Obshhie-metodicheskie-ukazaniya-po-VKR-SPO-PPSSZ.pdf

4. ПЕРЕЧЕНЬ РЕЗУЛЬТАТОВ, ДЕМОНСТРИРУЕМЫХ НА ГИА

Перечень результатов, демонстрируемых на ГИА (защита дипломной работы) для специальности 09.02.07 Информационные системы и программирование:

Оцениваемые основные виды деятельности и компетенции по ним	**Описание выполняемых в ходе процедур ГИА на защите ДР (примерная тематика дипломных работ)**
Защита дипломной работы	
Осуществление интеграции программных модулей: ПК 2.1. Разрабатывать требования к программным модулям на основе анализа проектной и технической документации на предмет взаимодействия компонент. ПК 2.2. Выполнять интеграцию модулей в программное обеспечение. ПК 2.3. Выполнять отладку программного модуля с использованием специализированных программных средств. ПК 2.4. Осуществлять разработку тестовых наборов и тестовых сценариев для программного обеспечения. ПК 2.5. Производить инспектирование компонент программного обеспечения на предмет соответствия стандартам кодирования.	Разработка программного обеспечения для автоматизации учета клиентов Разработка автоматизации системы учета клиентов в организации Разработка системы учета платежей предприятия для ООО «Формула управления» Проектирование автоматизированной информационной системы взаимодействия заказчика и исполнителя в логистической компании Разработка информационной системы корпоративного уведомления для ООО «Формула управления» Разработка автоматизации системы учета материалов в организации Автоматизированная обработка экономической информации по учету материальных ценностей в торговой компании Создание информационного сайта для сторонней организации в ООО «Формула Управления» Создание информационного сайта ООО «Формула Управления» Разработка автоматизированной информационной системы контроля и учета рабочего времени сотрудников компании Создание приложения для автоматизации учета данных компании Разработка программного обеспечения для автоматизации учета материалов Разработка цифровой образовательной среды на основе CMS "Moodle" Разработка пректа информационно-рекламного сайта сети ООО «Игралайф» Разработка сайта-визитки организации Разработка автоматизированной информационной системы кадровой службы Разработка интегрированной модели образовательного контента в системе СПО на базе системы «Moodle» Разработка информационного веб-сайта для
Ревьюирование программных продуктов: ПК 3.1. Осуществлять ревьюирование программного кода в соответствии с технической документацией. ПК 3.2. Выполнять процесс измерения характеристик компонент программного продукта для определения соответствия заданным критериям. ПК 3.3. Производить исследование созданного программного кода с использованием специализированных программных средств с целью выявления ошибок и отклонения от алгоритма. ПК 3.4. Проводить сравнительный анализ программных продуктов и средств разработки, с целью выявления наилучшего решения согласно критериям, определенным техническим заданием.	
Проектирование и разработка информационных систем: ПК 5.1. Собирать исходные данные для разработки проектной документации на информационную систему. ПК 5.2. Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика. ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием. ПК 5.4. Производить разработку модулей информационной системы в соответствии с	

техническим заданием. ПК 5.5. Осуществлять тестирование информационной системы на этапе опытной эксплуатации с фиксацией выявленных ошибок кодирования в разрабатываемых модулях информационной системы. ПК 5.6. Разрабатывать техническую документацию на эксплуатацию информационной системы. ПК 5.7. Производить оценку информационной системы для выявления возможности ее модернизации.	предприятия Разработка автоматизации системы документооборота в ООО «Гарант Сервис» Разработка приложения приема и учета заказов в ООО «Гарант Сервис»
Сопровождение информационных систем: ПК 6.1. Разрабатывать техническое задание на сопровождение информационной системы. ПК 6.2. Выполнять исправление ошибок в программном коде информационной системы. ПК 6.3. Разрабатывать обучающую документацию для пользователей информационной системы. ПК 6.4. Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания. ПК 6.5. Осуществлять техническое сопровождение, обновление и восстановление данных информационной системы в соответствии с техническим заданием.	
Соадминистрирование баз данных и серверов: ПК 7.1. Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов. ПК 7.2. Осуществлять администрирование отдельных компонент серверов. ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов. ПК 7.4. Осуществлять администрирование баз данных в рамках своей компетенции. ПК 7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации.	

ПРИЛОЖЕНИЕ 1

ОБРАЗЕЦ НАПИСАНИЯ ВВЕДЕНИЯ

Потребность в защите информации в современном Российском обществе существует не только у предприятий крупного и среднего бизнеса, но и у малого бизнеса. Регулярное появление новых угроз требует постоянного совершенствования защищённости любой организации, ведь в противном случае при реализации угрозы предприятию может быть нанесён непоправимый ущерб. Возможности малого бизнеса зачастую не позволяют организовать работу специальных служб, обеспечивающих информационную безопасность организации, осуществляющих выявление, предупреждение и устранение возникающих в ней угроз.

Малый бизнес является одним из наименее защищенных от угроз информационной безопасности в силу ряда причин:

1. Высокая стоимость средств защиты информации;
2. Потребность в привлечении сторонних квалифицированных специалистов в области ЗИ;
3. Недостаточное методическое обеспечение деятельности по разработке КСЗИ.

Актуальность данной работы заключается в создании комплексной системы защиты информации в ООО “…”.

Объектом дипломной работы является компьютерная фирма ООО “…”, занимающаяся продажей компьютеров и оргтехники для корпоративных клиентов и государственных структур.

Предметом дипломной работы является КСЗИ.

Целью ДР является создание комплексной системы мер по защите информации, составляющей коммерческую тайну ООО “…”.

В соответствии с поставленной целью необходимо решить следующие задачи:

1.Проанализировать информационную систему ООО “…” с точки зрения информационной безопасности;

2.Определить объекты защиты и привести теоретическое обоснование рекомендуемых средств защиты информации;

3.Разработать проект комплексной системы защиты информации ООО “…”;

4.Дать оценку экономической целесообразности реализации проекта КСЗИ в ООО “…”.

ПРИЛОЖЕНИЕ 2

ОБРАЗЕЦ НАПИСАНИЯ ЗАКЛЮЧЕНИЯ

В ходе выполнения ДР был произведен анализ существующих мер по защите информации на предприятии ООО “…”. В результате этого были выявлены угрозы, которые требуют устранения. На основании этого была разработана работа КСЗИ ООО “…”. Данная работа, включает в себя мероприятия, благодаря которым возможно устранение угроз и уязвимостей в данной организации.
В процессе выполнения данной ДР, было произведено обследование, которое включает в себя:

1. Разработку паспорта предприятия с точки зрения информационной безопасности – выявлена общая структура организации, информационная среда предприятия, программно - аппаратные средства, виды деятельности, виды защищаемой информации, конкуренты, описана строительная инфраструктура здания, определена контролируемая зона защищаемого помещения и объектов защиты информации, на которых обрабатывается информация ограниченного доступа.
2. Разработку модели деятельности предприятия – выявлены базовые бизнес – процессы, определены информационные потоки и информация ограниченного доступа циркулирующая на предприятии.
3. Описание информационной системы предприятия – выявлены характеристики АРМ, сервера и программное обеспечение, установленное на них, а также периферийные устройства.
4. Выявление объектов защиты – были выявлены объекты защиты, в которых обрабатывается и циркулирует информация ограниченного доступа.
5. Разработку модели угроз и уязвимостей для важных объектов защиты и расчет рисков для них – установлены угрозы и уязвимости для важных объектов защиты и вероятность их реализации, а также рассчитаны риски по выбранной методике ФСТЭК.

В результате установленной информации было разработано техническое задание на создание КСЗИ ООО “…”.

Были выявлены угрозы и уязвимости, с помощью которых может быть разглашена информация ограниченного доступа. В связи с этим, разработаны мероприятия затрудняющие или полностью исключающие реализацию угроз через уязвимости.
Была рассчитана экономическая целесообразность внедрения данной работы, по итогу которой было установлено, что создание КСЗИ в ООО “…” экономически целесообразно.

ПРИЛОЖЕНИЕ 3

ОБРАЗЕЦ НАПИСАНИЯ: глава 1 Теоретическая часть

ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Обзор возможных методов устранения уязвимостей

Важным этапом работы по созданию комплексной системы защиты информации является определение и анализ имеющихся мер, методов и средств, направленных на устранение выявленных у объектов защиты угроз и уязвимостей. На данном этапе работы необходимо определить наиболее эффективные пути решения поставленных задач.

2.2. Угрозы связанные с нарушением свойства информации

2.2.1. Разглашение, копирование, хищение информации ограниченного доступа. Данный тип угрозы реализуется посредством акустического, оптического и материального каналов утечки информации. Уязвимости, приводящие к возможной реализации данной угрозы:

1. Нарушение соглашения о неразглашении коммерческой тайны; 2.Несанкционированное проникновение в помещение; 3.Отсутствие режима коммерческой тайны.

Установленные уязвимости возможно устранить благодаря разработке организационно-распорядительной документации, включающей в себя: положение о режиме коммерческой тайны, перечень сведений составляющих коммерческую тайну, приказы об их утверждении. Для наилучшей эффективности устранения данных уязвимостей, необходимо провести беседу с сотрудниками организации, работающими с информацией ограниченного доступа с целью доведения требований по работе с ней и ответственности за её разглашение.

2.2.2. Уничтожение, модификация, блокировка носителей информации, АРМ сотрудников, серверного оборудования

К данному типу угроз относятся следующие уязвимости:

1.Несанкционированное проникновение в помещение;

2.Отсутствие мероприятий по повышению информационной грамотности;

3.Отсутствие инструкции по работе с АРМ и серверным оборудованием обрабатывающим коммерческую тайну;

4.Отсутствие учета носителей содержащих коммерческую тайну;

5.Отсутствие пломбирования корпуса АРМ.

В качестве решения по устранению данных уязвимостей, необходимо выполнение ряда мероприятий. Во-первых, необходимо установить средство контроля и управления доступом. Данное средство позволит организовать пропускной режим, благодаря которому ограничим доступ сотрудникам, не имеющим доступ к защищаемой информации. Во-вторых, необходимо через определённый промежуток времени проводить мероприятия по повышению информационной грамотности. Проводимые мероприятия позволят улучшить владение приемами поиска, сбора, обработки, анализа и синтеза необходимой информации. В-третьих, необходима инструкция по работе с АРМ и серверным оборудованием. В рамках данной дипломной работы, разработка данной инструкции не требуется. В-четвёртых, нанести на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя такой информации. Учет носителей позволит в любое время определить, у кого находиться тот или иной документ, содержащий информацию ограниченного доступа. В-пятых, произвести опломбировку системных блоков АРМ сотрудников и сервера, а также назначение ответственного за сохранность пломб. Данный способ позволит исключить физическое несанкционированное взаимодействие с носителями, содержащими коммерческую тайну.

2.3. Угрозы, связанные с НСД

В связи со стремительным развитием информационных технологий, большое количество организаций занимается обработкой информации ограниченного доступа в рамках своей информационной системы. В результате, в условиях высокой конкурентности, возрастает интерес сторонних компаний к информации ограниченного доступа своих конкурентов.

Несанкционированный доступ, служит одним из методов для получения сторонними организациями информации ограниченного доступа.

Несанкционированный доступ представляет собой противоправное действие, в результате которого злоумышленник получает доступ к защищаемой информации для сторонних лиц. На основании обследования, в рамках данной ДР были установлены следующие угрозы, связанные с несанкционированным доступом:

1.Несанкционированный доступ к АРМ сотрудников;

2.Угрозы несанкционированного доступа по каналам связи.

2.3.1. Несанкционированный доступ к АРМ сотрудников

Угроза несанкционированного доступа к АРМ сотрудников может быть реализована посредством следующих уязвимостей:

1.Отсутствие пломбирования корпуса АРМ;

2.Отсутствие регламента доступа к АРМ;

3.Отсутствие видеонаблюдения;

4.Отсутствие средств защиты от НСД.

Способ устранения первой уязвимости представлен в пункте 2.3. В качестве решения второй проблемы можно разработать матрицу доступа, в которой будет содержаться список лиц, допущенных к АРМ на которых обрабатывается информация ограниченного доступа. В рамках данной ДР, разработка матрицы доступа не требуется. Третью уязвимость можно устранить посредством внедрения на объекте видеонаблюдения. Видеонаблюдение предназначено для контроля сотрудников, имеющих доступ к информации ограниченного доступа, а также для выявления несанкционированного проникновения в помещение с конфиденциальной информацией. Для устранения четвёртой проблемы необходимо установить специальное программно-аппаратное средство защиты информации. Для этого необходимо сравнить сертифицированные СЗИ от НСД.

Таблица № – Сравнение средств защиты от НСД

Критерии сравнения	Secret Net 7	Dallas Lock 8.0 – K	Страж NT 4.0	СЗИ Аура 1.2.4

Таким образом, на основании данного анализа СЗИ от НСД было выбрано СЗИ "Аура 1.2.4". Данный выбор был связан с низкой стоимостью продукта и удовлетворением функциональными возможностями продукта. СЗИ "Аура 1.2.4" позволяет обеспечить идентификацию и аутентификацию автоматизированных рабочих мест сотрудников, а также разграничить доступ к устройствам и защищаемой информации, путем применения политики доступа. Скриншоты настроек представлены в приложении №.

2.3.2. Угрозы несанкционированного доступа по каналам связи.

У данного вида угрозы выявлены следующие уязвимости:

1.Анализ сетевого трафика;

2.Сканирование сети;

3.Выявление паролей;

4.Получение НСД путем подмены доверенного объекта;

5.Отказ в обслуживании.

Первые две проблемы связанными с анализом сетевого трафика и сканированием сети имеют малую вероятность реализации. Это связано с тем что в организации установлен

антивирус включающий в себя защиту от данных уязвимостей. Таким образом, в рамках ДР устранение данных уязвимостей не требуется. Проблему связанной с выявлением паролей можно устранить путем реализации одноразовых паролей. Данный способ является эффективным от подсматривания паролей другими сотрудниками. Четвёртая уязвимость может быть ликвидирована путём грамотной настройки управлением доступа. Уязвимость типа отказа в обслуживании могут сделать сеть организации недоступной. Таким образом во избежание этого необходимо настроить виртуальную внутреннюю сеть, позволяющей ликвидировать выявленную уязвимость.

Выводы по второй главе

На основании выявленных угроз информационной безопасности в организации ООО "…", в рамках ДР, был разработан комплекс мероприятий, направленных на минимизацию вероятности реализации выявленных угроз:

1. От угрозы, связанной с разглашением, копированием, хищением информации ограниченного доступа: разработка организационно-распорядительной документации по защите информации, составляющей коммерческую тайну в организации; проведение беседы с сотрудниками организации для ознакомления под расписку с требованиями по работе с защищаемой информации.
2. От угрозы, связанной с уничтожением, модификацией, блокировкой, хищением носителей информации, АРМ сотрудников, серверного оборудования: установка средства контроля управлением доступа; проведение мероприятий по повышению информационной грамотности персонала; разработка инструкции по работе с АРМ и серверным оборудованием; нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна"; опломбировка системных блоков автоматизированных рабочих мест сотрудников и сервера, а так же назначение ответственного за их сохранность.
3. От угрозы, связанной с несанкционированным доступом к АРМ сотрудников: разработка матрицы доступа; внедрение в организации видеонаблюдения; установка СЗИ от НСД " Аура 1.2.4";
4. От угрозы, связанной с несанкционированным доступом по каналам связи: использование одноразовых паролей; настройка управления доступом; настройка виртуальной внутренней сети организации.

Результаты теоретического обоснования выбора средств защиты для реализации КСЗИ ООО "…", легли в основу разработки ДР.