МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Программа итоговой (государственной итоговой) аттестации, как компонент образовательной программы
высшего образования - программа специалитета по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ) Тимониным В.С.

ПРОГРАММА ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ

ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Специальность:	10.05.01 Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	Очная

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2023

Программа итоговой (государственной итоговой) аттестации в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

1. Итоговая (государственная итоговая) аттестация по специальности 10.05.01 Компьютерная безопасность и специализации Информационная безопасность объектов информатизации на базе компьютерных систем в соответствии с учебным планом проводится в форме: Защиты выпускной квалификационной работы.

2. Выпускная квалификационная работа.

2.1. Вид выпускной квалификационной работы: Дипломный проект

2.2. Требования к выпускной квалификационной работе.

Государственная итоговая аттестация по специальности 10.05.01 Компьютерная безопасность в соответствии с решением Ученого совета университета включает в себя:

Государственная итоговая аттестация по специальности 10.05.01 – «Компьютерная безопасность» в соответствии с п.6.8 ФГОС ВО и решением Ученого совета вуза включает в себя защиту выпускной квалификационной работы (дипломного проекта) Государственный экзамен по направлению не предусмотрен учебной программой. Трудоемкость итоговой (государственной) аттестации: 9 зет (324 часа)

2.3. Порядок выполнения выпускной квалификационной работы.

Дипломный проект представляется к защите в виде двух основных частей: - расчетно-пояснительной записки; - иллюстрированного (графического) материала. Требования к расчетно-пояснительной записке следующие: - полное соответствие теме; - содержательность, четкость изложения; - логическая последовательность излагаемого материала; - убедительность аргументации; - точность формулировок, исключающая возможность неоднозначного толкования; - конкретность изложения результатов дипломного проекта с четким указанием собственного вклада; - доказательность выводов и обоснованность рекомендаций; - система ссылок на источники текстов, графики, формул, качественных и экспертных оценок. 3.1. Расчетно-пояснительная записка представляется на кафедру в двух версиях - в виде переплетенной распечатки (формат А4) и на компакт-диске CD-RW. 3.2. Объем расчетно-пояснительной записки (без приложений) должен составлять не более 80 страниц текста (не считая рисунков и таблиц). Следует использовать 14-й шрифт с полуторным межстрочным интервалом. Типовая структура расчетно-пояснительной записки типового дипломного

проекта представлена в таблице 1. Графическая часть дипломного проекта в пояснительной записке представляется только исключительно в компьютерном исполнении и содержит обычно 6-8 листов формата А1. Примерное содержание графического материала (с учетом выбранной темы) представлено в таблице 2. (Приложение) 4. Содержание расчетно-пояснительной записки В состав расчетно-пояснительной записки дипломного проекта входят разделы, соответствующие по названию разделам пункта 4 ЗДП «Содержание пояснительной

записки» с добавлением разделов «Аннотация», «Литература», «Приложения». 1. Аннотация должна содержать краткую характеристику содержания дипломного проекта с указанием наиболее важных задач, которые решены автором в данном дипломном проекте. 2. В разделе «Введение» введении должно быть изложено обоснование актуальности темы проекта, сформулирована цель работы и указаны основные задачи, которые при этом необходимо решать. Задачи формулируют таким образом, чтобы описание их решения составило содержание разделов основной части дипломного проекта. Во введении также необходимо отметить научную работу новизну и практическую значимость вашего проекта. Введение должно «вводить» в дипломный проект. 3. В разделе «Характеристика объекта информатизации» необходимо дать всестороннюю характеристику тому объекту, для которого требуется разработать систему защиты. Можно представить структурно-функциональную схему объекта информатизации. Охарактеризовать средства, способы, методы хранения, обработки и передачи информации, дать характеристику программно-технической «среды» рассматриваемой КС или сети. Выявить недостатки существующей системы защиты информации объекта информатизации. 4. В разделах «Анализ и оценка текущего состояния защищенности объекта» необходимо отразить процесс получения и выявления объективных данных о текущем состоянии системы защиты информации объекта. При этом необходимо провести анализ использованной на защищаемом объекте информации, определить ее виды, гриф и степень секретности, ценность. Выдать все виды угроз и возможные атаки на защищаемый объект. 5. Определение требований к КСЗИ объекта. В этом разделе, исходя из результатов(проведенных ранее) анализа ценности информации, возможных каналов ее утечки и угроз, необходимо сформулировать требования к КСЗИ объекта: - общие требования; - требования по техническому, программному и программно-техническому обеспечению; - нормативно-правовые и административные; - специальные требования; - требования к способам и средствам защиты компьютерных систем и сетей; - требования к режимам обработки информации. На основе

указанных требований разработать направления и этапность проведения работ по созданию КСЗИ. 6. Обоснование выбора средств защиты информации. В данном разделе необходимо дать обоснованный выбор методов, правовых и инженерно-технических решений, аппаратно-программных, криптографических средств и организационных мероприятий по обеспечению, целостности и сохранности защищаемой на объекте, информации. 7. Разработка КСЗИ и мероприятий по ее внедрению. Данный раздел является ключевым в дипломном проекте и должен содержать: - структурно-функциональную схему, предлагаемой Вами системы защиты, и отражающую требуемый уровень защищенности объекта информатизации;

- алгоритмы используемых методов и средств (криптографических, аппаратно-программных, организационных и др.) разрабатываемой КСЗИ; - современные технологии для обеспечения информационной безопасности компьютерных систем; - программы – методики испытаний систем защиты информации и технические регламенты для сопровождения КСЗИ на объекте. 8. Разработка организационной структуры службы безопасности объекта. В данном разделе должна быть обоснована и предложена организационная структура, обеспечивающая требуемый уровень защищенности объекта в зависимости от особенностей обработки информации и размерности системы. Этой структурой может быть: группа, отдел или отдельная служба. Необходимо дать обоснование численного состава данных подразделений, а также разработать должностные инструкции сотрудников и другие нормативные документы. 9. Экономическая часть. В данном разделе следует выполнить экономическое обоснование выбора отдельных компонентов КСЗИ объекта с указанием фирм-поставщиков оборудования и программного обеспечения.

2.4. Примерный перечень тем выпускных квалификационных работ.

Сравнительный анализ средств защиты информации в ОС (Windows, Unix)

Разработка алгоритмов обнаружения вторжения в информационную сеть компаний IPG

Разработка регламента обеспечения защиты персональных данных в ГВЦ ОАО «РЖД»

Система мониторинга и обнаружения инцидентов безопасности компании ПКБ ЦТ ОАО «РЖД»

Разработка средств защиты объектов информации КС органов государственного управления

Разработка средств защиты тракта передачи информации между АРМ и БД платежной банк-системы

Защита конфиденциальной информации от внутренних угроз на примере ОАО «Первобанк»

Разработка алгоритмов защиты от dos/ddos атак на ЛВС предприятия

Защита информации от инсайдерских атак в корпоративной сети предприятий железнодорожного транспорта

Информационная защита инфраструктуры систем «online» оповещения

Разработка алгоритма защиты интернет – портала от MYSQL-инъекций

Защита персональных данных в КС железнодорожного транспортного предприятия

Реализация средств обеспечения ИБ БД при использовании системы «тонкого клиента»

Разработка алгоритма мониторинга обеспечения защищенности КС ж.д. транспорта

Применение средств системы управления контентом для обеспечения ИБ портала

Внедрение программного комплекса AVANPOST для управления доступом к ресурсам корпоративной сети компании

Защита персональных данных в корпоративной сети предприятия

Разработка защиты информации в корпоративной сети на базе MPLS

Обеспечение целостности и сохранности БД корпоративной сети

Внедрение программно-аппаратного комплекса компании CISCO в КС предприятия для защиты от внутренних угроз

Защита информации в корпоративной сети на основе технологии Kerberos

Разработка метода защиты мультимедийной информации

Разработка программного комплекса анализа уязвимостей программного обеспечения

Разработка лабораторной реализации корпоративной виртуальной частной сети

Разработка модели программной защиты в операционных системах

Разработка информационной системы поддержки проектирования подсистем защиты информации объектов критической информационной инфраструктуры 3 категории

Разработка модели обнаружения уязвимостей компьютерных систем

Разработка системы поддержки обнаружения недекларированных возможностей систем управления

Разработка анализатора защиты периметра локальной сети предприятия

Разработка системы защиты информации корпоративных порталов

Разработка методики встраивания QR-кода в алгоритм двухфакторной аутентификации

Разработка методики сбора информации с открытых веб-источников

Разработка методического обеспечения учебной дисциплины «Стеганографические методы защиты информации»

Разработка методики нахождения и регистрации уязвимостей веб-приложений

Разработка распределенной системы обеспечения целостности информации

Разработка системы правил для обеспечения безопасности удаленного доступа к информационным ресурсам с применением системы унифицированного управления конечными устройствами

Методика перевода системы защиты информационной безопасности корпоративной сети АО «РЖДСтрой» на отечественное ПО

Разработка методики встраивания хэш-функции «Стрибог» в протокол TLS 1.3

Разработка модели защиты информации на основе изолированной программной среды

Разработка дискреционной модели защиты информации в корпоративной сети предприятия

Разработка классификаторов реагирования dlp системы для определения инцидентов безопасности при обработке конфиденциальной информации на предприятиях железнодорожного транспорта

Разработка прототипа информационной системы поддержки деятельности по технической защите конфиденциальной информации

Разработка проекта модернизации подсистемы информационной безопасности корпоративной сети ОАО «РЖД»

Разработка методики встраивания шифра «Магма» в протокол TLS 1.3

Разработка программных роботов для оптимизации рутинных операций ОАО "РЖД"

Разработка системы обеспечения компьютерной безопасности при роботизации бизнес-процессов

Разработка методики и способов защиты исходного кода и информации, размещаемой в одностраничных web-приложениях и на web-сайтах

Разработка методики обнаружения атак на компьютерные сети при помощи нейронных сетей

Разработка методики внедрения кибериммунного подхода в решении задач информационной безопасности в транспортной отрасли

Разработка методики обеспечения безопасности сети предприятия с использованием криптошлюза "Континент"

Разработка модели выявления уязвимостей исходного кода на предприятии и ее интеграция с хранилищем

Автоматизированная система замены преподавателей по болезни

Разработка анализатора уязвимостей исходного кода с использованием методологии DevSecOps

Разработка модели импульсной нейронной сети предотвращения низкоинтенсивной ddos - атаки

Разработка лабораторного стенда для создания тестовой сети государственной информационной системы 1 класса защищенности на основе программно-аппаратного комплекса "Рубикон-А"

Разработка модели сверточной нейронной сети предотвращения ddos - атаки

Разработка виртуальной частной сети малого предприятия

Совершенствование процесса авторизации на веб-сервисах по протоколу OAuth2.0

3. Перечень компетенций, которые должны быть сформированы у обучающихся в результате освоения образовательной программы.

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-2 - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-4 - Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;

ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-7 - Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-11 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

ОПК-12 - Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;

ОПК-13 - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;

ОПК-14 - Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;

ОПК-15 - Способен администрировать компьютерные сети и контролировать корректность их функционирования;

ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

ОПК-17 - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

ПК-1 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах;

ПК-2 - Способен применять математические методы в области компьютерной безопасности;

ПК-3 - Способен проводить анализ исходных данных и формировать требования к компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности;

ПК-4 - Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных средств защиты информации, защищенных операционных систем, систем управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации;

ПК-5 - Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты;

ПК-6 - Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-7 - Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;

ПК-8 - Способен проводить инструментальный мониторинг защищенности компьютерных систем;

ПК-9 - Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию;

ПК-10 - Способен организовать процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПК-11 - Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации;

ПК-12 - Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах;

ПК-13 - Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

ПК-14 - Способен проводить моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации;

ПК-15 - Способен принимать участие в разработке проектных решений по защите информации в автоматизированных системах;

ПК-16 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем;

ПК-17 - Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации;

ПК-18 - Способен принимать участие в разработке архитектуры системы защиты информации автоматизированной системы;

ПК-19 - Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

ПК-20 - Способен подготовить обоснование необходимости защиты информации в автоматизированной системе;

ПК-21 - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

ПК-22 - Способен проводить тестирование систем защиты информации автоматизированных систем;

ПК-23 - Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем;

ПК-24 - Способен разрабатывать модели угроз, формировать требования по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-25 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-26 - Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-27 - Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем;

ПК-28 - Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла;

УК-3 - Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

УК-4 - Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия;

УК-5 - Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия;

УК-6 - Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;

УК-7 - Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;

УК-8 - Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в

том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов;

УК-9 - Способен использовать базовые дефектологические знания в социальной и профессиональной сферах;

УК-10 - Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;

УК-11 - Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности.

4. Критерии оценки результатов итоговой (государственной итоговой) аттестации.

Критерии оценки результатов защиты выпускной квалификационной работы

Шкала оценивания	Критерии

Авторы:

профессор, профессор, д.н. кафедры «Управление и защита информации» М.Я. Клепцов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин