Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ
Директор ИУАТ

Король Р.Г.

23.05.2025

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Преддипломная практика

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): к.т.н., доцент, Ешенко Роман Анатольевич;к.т.н., доцент, Попов Михаил Алексеевич

Обсуждена на заседании кафедры: (к202) Информационные технологии и системы

Протокол от 14.05.2025г. № 5

Обсуждена на заседании методической комиссии по родственным направлениям и специальностям:

Протокол от 23.05.2025 г. № 4

г. Хабаровск
2025 г.

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2028 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2029 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2029 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Программа Преддипломная практика

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1457

Квалификация **специалист по защите информации**

Форма обучения **очная**

ОБЪЕМ ПРАКТИКИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЁ ПРОДОЛЖИТЕЛЬНОСТЬ В НЕДЕЛЯХ И В АКАДЕМИЧЕСКИХ ЧАСАХ

Общая трудоемкость **17 ЗЕТ**

Продолжительность **11,33 нед.**

Часов по учебному плану 612 Виды контроля в семестрах:

в том числе: зачёты с оценкой 11

контактная работа 2

самостоятельная работа 606

Распределение часов

Семестр (<Курс>.<Семестр на курсе>)	**11 (6.1)**		Итого	
Недель				
Вид занятий	УП	РП	УП	РП
Лекции	2	2	2	2
Контроль самостоятельной работы	4	4	4	4
Итого ауд.	2	2	2	2
Контактная работа	6	6	6	6
Сам. работа	606	606	606	606
Итого	612	612	612	612

1. ВИД ПРАКТИКИ, СПОСОБ И ФОРМА (ФОРМЫ) ЕЁ ПРОВЕДЕНИЯ	
1.1	Тип практики: преддипломная. Вид практики: производственная. Способы проведения практики: стационарная, выездная. Форма проведения практики: дискретно.
1.2	Целью преддипломной практики является приобретение студентом опыта в исследовании актуальной научной проблемы или решении реальной задачи. Данная цель может быть достигнута за счет изучения студентом реальных условий деятельности организации. Большая часть преддипломной практики посвящена сбору материалов для выпускной квалификационной работы.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б2.О.03(Пд)
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Научно-исследовательская работа
2.1.2	Информационные системы на железнодорожном транспорте
2.1.3	Научно-исследовательская работа
2.1.4	Основы научных исследований
2.1.5	Программно-аппаратные средства защиты информации
2.1.6	Техническая защита информации и средства контроля
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Научно-исследовательская работа

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

Знать:

Методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации

Уметь:

Применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации.

Владеть:

Методологией системного и критического анализа проблемных ситуаций; методиками постановки цели, определения способов ее достижения, разработки стратегий действий.

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

Знать:

Этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами.

Уметь:

Разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ; объяснить цели и формулировать задачи, связанные с подготовкой и реализацией проекта; управлять проектом на всех этапах его жизненного цикла.

Владеть:

Методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта

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

Знать:

Правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном языках; существующие профессиональные сообщества для профессионального взаимодействия.

Уметь:

Применять на практике коммуникативные технологии, общения для академического и профессионального взаимодействия.

Владеть:

Методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий.

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

Знать:
Методики самооценки, самоконтроля и саморазвития с использованием подходов здоровьесбережения.
Уметь:
Решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности.
Владеть:
Технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровьесберегающих подходов и методик.

УК-9: Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
Знать:
Законодательство РФ в области экономической и финансовой грамотности и систему финансовых институтов в РФ
Уметь:
Оценивать степень риска продуктов и услуг финансовых институтов и на основании этого принимать обоснованные экономические решения
Владеть:
Навыками грамотно определять финансовые цели в различных областях жизнедеятельности на основе сбора и анализа финансовой информации

ОПК-2: Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;
Знать:
состав, классификацию, особенности функционирования программных средств системного и прикладного назначений
Уметь:
рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности
Владеть:
навыками использования системного программного обеспечения для решения задач профессиональной деятельности; навыками использования прикладного программного обеспечения для решения задач профессиональной деятельности

ОПК-3: Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;
Знать:
математические методы, необходимые для решения задач профессиональной деятельности
Уметь:
использовать типовые математические методы и модели для решения задач профессиональной деятельности
Владеть:
подходами к решению стандартных расчетов математических величин, применению математических методов обработки экспериментальных данных для 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;
Знать:
основные понятия и законы физики. основы микроэлектронной техники
Уметь:
использовать физические законы, анализировать и применять модели явлений, процессов и объектов (включая схемы электронных устройств) при решении инженерных задач в профессиональной деятельности
Владеть:
основными методами теоретического и экспериментального исследования физических явлений и процессов, в том числе лежащих в основе микроэлектронной техники

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;
Знать:
состав и содержание Российских и международных нормативных правовых актов, нормативных и методических документов, межгосударственных и международных стандартов, регламентирующих деятельность по защите информации

Уметь:

применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации

Владеть:

методами поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации

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

Знать:

содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации; правовые и организационные меры защиты информации, в том числе информации ограниченного доступа, в автоматизированных системах.

Уметь:

разрабатывать организационнораспорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах

Владеть:

способами применения действующуей нормативной базы в области защиты информации ограниченного доступа в автоматизированных системах

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

Знать:

алгоритмические основы программирования на языках общего назначения; языки программирования общего назначения; методы, реализуемые в современных инструментальных средствах программирования

Уметь:

осуществлять обоснованный выбор способов организации программ и инструментария программирования при решении профессиональных задач

Владеть:

навыками разработки алгоритмов для последующего создания программ на языках общего назначения; навыками использования типовых инструментальных средств
программирования для решения профессиональных задач

ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;

Знать:

текущее состояние и тенденции развития методов и средств защиты информации от утечки по техническим каналам; особенности построения, функционирования и защитысовременных распределенных информационных систем и их коммуникационной среды: особенности построения, функционирования и защиты информации в современных центрах обработки данных

Уметь:

проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурнотехнических решений, реализованных при построении
ЭВМ и систем; применять средства защиты от утечки по техническим каналам при решении задач профессиональной деятельности. определять требования по защите
коммуникационной среды распределенной информационной системы

Владеть:

навыками реализации вычислительных процедур на микропрограммном уровне при решении задач профессиональной деятельности; методами проектирования и
навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности и проектирования распределенных информационных систем, в том числе разработки приложений, реализующих параллельные вычисления

ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

Знать:

основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в

автоматизированных системах и систем электронного документооборота
Уметь:
разрабатывать и анализировать программные модели средств криптографической защиты информации
Владеть:
навыками использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач

ОПК-11: Способен разрабатывать компоненты систем защиты информации автоматизированных систем;
Знать:
программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем
Уметь:
разрабатывать компоненты защиты информации автоматизированных систем
Владеть:
навыками применения инструментальных средств поддержки всех этапов разработки компонентов систем защиты информации автоматизированных систем навыками применения программных и аппаратных компонентов, разрабатываемых различными фирмамипроизводителями, при построении систем защиты информации

ОПК-12: Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;
Знать:
принципы построения и функционирования, основы обеспечения информационной безопасности вычислительных сетей, базовые средства защиты современных операционных систем и баз данных
Уметь:
применять знания в области безопасности вычислительных сетей, операционных систем, систем баз данных, при разработке автоматизированных систем
Владеть:
навыками применения основных средств обеспечения безопасности вычислительных сетей навыками использования функциональных возможностей, в том числе средств администрирования, операционных систем для решения задач профессиональной деятельности навыками проектирования, разработки и эксплуатации баз данных

ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;
Знать:
основы диагностики и тестирования систем защиты информации автоматизированных систем базовые методы анализа уязвимостей систем защиты информации и моделирования угроз информационной безопасности автоматизированных систем
Уметь:
проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем
Владеть:
базовыми навыками проведения диагностики и тестирования систем защиты информации автоматизированных систем

ОПК-14: Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;
Знать:
основные методы управления проектами в области информационной безопасности
Уметь:
разрабатывать, внедрять в эксплуатацию, оценивать качество автоматизированных систем; проводить подготовку исходных данных для техникоэкономического обоснования проектных решений
Владеть:
базовыми методами проектирования, разработки, внедрения в эксплуатацию автоматизированных систем в защищенном исполнении

ОПК-16: 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.

Знать:
основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире
Уметь:
формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории
Владеть:
принципами историзма и научной объективности как основой формирования собственной гражданской позиции и развития патриотизма

ОПК-9.2.: Способен осуществлять внедрение и эксплуатацию систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам);
Знать:
особенности эксплуатации систем защиты информации автоматизированных систем на транспорте особенности эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте
Уметь:
осуществлять внедрение систем защиты информации автоматизированных систем на транспорте осуществлять внедрение систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами
Владеть:
методами эксплуатации систем защиты информации автоматизированных систем на транспорте методами эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами

ОПК-9.3.: Способен осуществлять контроль защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом установленных требований безопасности;
Знать:
основные угрозы и уязвимости, методы контроля защищенности автоматизированных систем на транспорте и методы контроля защищенности информационноуправляющих и информационнологистических систем на транспорте
Уметь:
выявлять уязвимости в автоматизированных системах на транспорте и в информационноуправляющих и информационнологистических системах на транспорте, в том числе в автоматизированных системах управления технологическими процессами; анализировать, прогнозировать и устранять угрозы информационной безопасности в течение всего времени их применения
Владеть:
навыками применения автоматизированных средств контроля защищенности автоматизированных систем на транспорте и контроля защищенности информационноуправляющих и информационно-логистических систем на транспорте

4. СОДЕРЖАНИЕ ПРАКТИКИ С УКАЗАНИЕМ ОТВЕДЕННОГО КОЛИЧЕСТВА ЧАСОВ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Самостоятельная работа						
1.1	Первичный инструктаж по ТБ /Лек/	11	2	УК-1		0	
1.2	Изучение организационной структуры и деловых процессов предприятия. /Ср/	11	50	УК-1 УК-2 УК-4 УК-6 УК-9 ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.3	Изучение содержания и структуры информационных потоков. /Ср/	11	50	УК-1 УК-2 УК-4 УК-6 УК-9 ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	

1.4	Изучение форм хранения информации. /Ср/	11	60	УК-1 УК-2 УК-4 ОПК-3 ОПК-4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.5	Проектирование бизнес-процессов и структуры информационной системы. /Ср/	11	60	УК-1 УК-2 УК-4 УК-6 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-9 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-9.2. ОПК-9.3. ОПК-16	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.6	Проектирование структуры базы данных. /Ср/	11	50	УК-1 ОПК-2 ОПК-3 ОПК-10 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-9.2. ОПК-9.3. ОПК-16	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.7	Обеспечение защиты базы данных от инсайдерских атак. /Ср/	11	50	УК-1 ОПК-2 ОПК-3 ОПК-5 ОПК-6 ОПК-10 ОПК-11 ОПК-12	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.8	Разработка интерфейса корпоративного приложения. /Ср/	11	66	УК-1 УК-4 УК-6 УК-9 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-9 ОПК-10 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-9.2. ОПК-9.3. ОПК-16	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.9	Оценка экономической эффективности разработки информационной системы и обеспечения её безопасности. /Ср/	11	60	УК-1 ОПК-10 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-9.2. ОПК-9.3. ОПК-16	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	

1.10	Разработка мероприятий по обеспечению безопасности труда. /Ср/	11	60	УК-1 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-9.2. ОПК-16	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.11	Оформление отчета по преддипломной практике. /Ср/	11	92	УК-1 УК-2 УК-4 УК-6 УК-9 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-9 ОПК-10 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-9.2. ОПК-9.3. ОПК-16	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3	0	
1.12	Дифференцированный зачет /ЗачётСОц/	11	8	УК-1 УК-2 УК-4 УК-6 УК-9 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-9 ОПК-10 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-9.2. ОПК-9.3. ОПК-16	Л1.1 Л1.2Л2.1 Л2.2	0	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

Размещены в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для проведения практики

	Авторы, составители	Заглавие	Издательство, год
Л1.1		Дипломное проектирование	Самара: Самарский государственный архитектурно-строительный университет, 2012, http://biblioclub.ru/index.php?page=book&id=142914
Л1.2		Дипломное проектирование	Астрахань: Астраханский инженерно-строительный институт, 2014, http://biblioclub.ru/index.php?page=book&id=438916

6.1.2. Перечень дополнительной литературы, необходимой для проведения практики

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Тарануха Н.А., Каменских И.В.	Разработка дипломного проекта для транспортных специальностей вузов. Требования, рекомендации, СПРАВОЧНЫЕ МАТЕРИАЛЫ: учеб. пособие	Москва: СОЛОН-Пресс, 2008,
Л2.2	Куликов В.П.	Дипломное проектирование. Правила написания и оформления: учеб. пособие	М.: ФОРУМ, 2008,

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для проведения практики

Э1	ИНТУИТ. Национальный открытый университет	http://www.intuit.ru
Э2	Научная электронная библиотека "КИБЕРЛЕНИНКА"	http://cyberleninka.ru
Э3	Электронные журналы, электронные книги, электронные справочники электронного ресурса издательства ЭБС "Университетская библиотека"	URL:http:/biblioclu

6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

6.3.1.1	ABBYY FineReader 11 Corporate Edition - Программа для распознавания текста, договор СЛ-46
6.3.1.2	ПО CorelDRAW Graphics Suite X6 Education License - Графический пакет, контракт 214
6.3.1.3	Office Pro Plus 2007 - Пакет офисных программ, лиц.45525415
6.3.1.4	Visio Pro 2007 - Векторный графический редактор, редактор диаграмм и блок-схем, лиц.45525415
6.3.1.5	Windows 7 Pro - Операционная система, лиц. 60618367
6.3.1.6	Free Conference Call (свободная лицензия)
6.3.1.7	Zoom (свободная лицензия)
6.3.1.8	LibreOffce - офисный пакет

6.3.2 Перечень информационных справочных систем

6.3.2.1	Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Аудитория	Назначение	Оснащение
424	Учебная аудитория для проведения лекционных, лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. "Основы информационной безопасности".	комплект учебной мебели, доска маркерная, проектор Windows 7 Pro Номер лицензии: 60618367 Контракт 208 ДВГУПС от 09.07.2012 бессрочная Office Pro Plus 2007 Номера лицензий: 45525415 (ГК 111 от 22.04.2009, бессрочная), 46107380 (Счет 00000000002802 от 14.11.07, бессрочная)
207	Учебная аудитория для проведения лабораторных и практических занятий. Лаборатория "Специальных информационных и автоматизированных систем".	Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС. Лицензионное программное обеспечение: Windows 10 Pro - MS DreamSpark 700594875, 7-Zip 16.02 (x64) - Свободное ПО, Autodesk 3ds Max 2021, Autodesk AutoCAD 2021, Autodesk AutoCAD Architecture 2021, Autodesk Inventor 2021, Autodesk Revit 2021- Для учебных заведений предоставляется бесплатно, Foxit Reader- Свободное ПО, MATLAB R2013b - Контракт 410 от 10.08.2015, Microsoft Office Профессиональный плюс 2007 - 43107380, Microsoft Visio профессиональный 2013 - MS DreamSpark 700594875, Microsoft Visual Studio Enterprise 2017- MS DreamSpark 700594875, Mozilla Firefox 99.0.1 - Свободное ПО, Opera Stable 38.0.2220.41 - Свободное ПО, PTC Mathcad Prime 3.0 - Контракт 410 от 10.08.2015 лиц. 3A1874498, КОМПАС-3D V19 - КАД-19-0909, АСТ-Тест лиц. АСТ.РМ.А096.Л08018.04, Договор № Л-128/21 от 01.06.2021 с 01 июля 2021 по 30 июня 2022. комплект учебной мебели, доска маркерная, проектор Windows 10 Pro Электронные ключи Контракт 1044 ДВГУПС от 25.11.2019 бессрочная Office Pro Plus 2007 Номера лицензий: 45525415 (ГК 111 от 22.04.2009, бессрочная), 46107380 (Счет 00000000002802 от 14.11.07, бессрочная)

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Преддипломная практика студента осуществляется в форме проведения реального разрабатываемого проекта,

выполняемого студентом в рамках задания руководителя ВКР по направлению обучения и предполагает выполнение студентом реализацию проектной части темы ВКР с учетом интересов и возможностей подразделений организации, в которых она проводится.
Преддипломная работа может проходить в любой организации соответствующей направлению обучения студента.

Содержание преддипломной работы определяется руководителем программы подготовки специалистов на основе ФГОС ВО и отражается в индивидуальном задании на преддипломную практику.

Индивидуальное задание может содержать следующие этапы:
1. Прохождение инструктажа по технике безопасности.
2. Работа с литературными источниками по теме ВКР.
3. Выбор и разработка методов решения поставленной задачи в рамках ВКР.
4. Разработка концепции проекта системы информационной безопасности.
5. Выбор инструментальных средств для разработки системы информационной безопасности.
6. Проектирование структуры базы данных.
7. Разработка модуля системы информационной безопасности.
8. Оформление отчета по практике.

Тематика исследований должна соответствовать научным направления работы кафедры «Информационные технологии и системы», а также отвечать задачам, имеющим теоретическое, практической, прикладное значение для различных отраслей народного хозяйства.
В каждом конкретном случае программа преддипломной практики изменяется и дополняется для каждого студента в зависимости от характера выполняемой работы.
Преддипломная практика студента оценивается на основе представленных отчетов.
Отчет сдается студентом на выпускающую кафедру за подписью научного руководителя.
К числу специальных требований, учитываемых при оценке НИР, относятся:
– владение методологией и современной проблематикой данной отрасли знания;
– владение компетенциями обучающимся, формируемыми в результате освоения практики;
– умение проектировать, внедрять и работать с конкретными программными продуктами, информационными ресурсами и техническими средствами защиты информации.

Оформленный отчет по преддипломной практике должен соответствовать следующим требованиям:
1. Отчет оформляется в текстовом редакторе MS Word на листах формата А4 (297х210).
2. Отчет должен быть отпечатан на компьютере через 1-1,5 интервала, номер шрифта – 12-14 пт Times New Roman. Расположение текста должно обеспечивать соблюдение следующих полей:
− левое 20 мм.
− правое 15 мм.
− верхнее 20 мм.
− нижнее 25 мм.
3. Все страницы отчета, включая иллюстрации и приложения, имеют сквозную нумерацию без пропусков, повторений, литературных добавлений. Первой страницей считается титульный лист, на которой номер страницы не ставится.
4. Таблицы и диаграммы, созданные в MS Excel, вставляются в текст в виде динамической ссылки на источник через специальную вставку.
5. Основной текст делится на главы и параграфы. Главы нумеруются арабскими цифрами в пределах всей работы и начинаются с новой страницы.
6. Подчеркивать, переносить слова в заголовках и тексте нельзя. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.
7. Ссылки на литературный источник в тексте сопровождаются порядковым номером, под которым этот источник включен в список используемой литературы. Перекрестная ссылка заключается в квадратные скобки. Допускаются постраничные сноски с фиксированием источника в нижнем поле листа.
8. Составление библиографического списка используемой литературы осуществляется в соответствии с ГОСТ.

К отчету также должны прилагаться:
- дневник практики (с указанием даты и проводимых мероприятиях за каждый день);
- отзыв от руководителя практики в организации;
- характеристика от руководителя практики в ДВГУПС;
- путевка (если практика проходит не в ДВГУПС);
- приказ от предприятия о назначении на должность (желательно).

Оформление и защита производится в соответствии со стандартом ДВГУПС СТ 02-11-17 «Учебные студенческие работы. Общие положения»
Оценка знаний по дисциплине производится в соответствии со стандартом ДВГУПС СТ 02-28-14
«Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации»

На основании отчета и защиты преддиплоной практики выставляется зачет с оценкой.

Оценочные материалы при формировании программ практик

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация: специализация N 9 "Безопасность автоматизированных систем на транспорте" (по видам)

Название практики: Преддипломная практика

Формируемые компетенции:

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при защите отчета по практике

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Экзамен или зачет с оценкой
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо

Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

Описание шкал оценивания
Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительн	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстриро-вать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной	Обучающийся демонстрирует способность к самостоятельно-му применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень контрольных вопросов и заданий на практику

Примерный перечень контрольных вопросов

Компетенции УК-1, УК-2, УК-4, УК-6, УК-9, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-?\7, ОПК-8, ОПК-9, ОПК-10, ОПК-11, ОПК-142, ОПК-13, ОПК-14, ОПК-16, ОПК-9.2, ОПК-9.3:

Раздел 1. Методология научного исследования.

Основания методологии науки. Характеристика научной деятельности. Средства и методы научного исследования. Организация процесса проведения исследования. Организация коллективного научного исследования.

Вопросы по разделу.

1. Философско-психологические и системотехнические основания.
2. Науковедческие основания.
3. Особенности научной деятельности.
4. Принципы научного познания.
5. Средства научного исследования.
6. Методы научного исследования.
7. Фаза проектирования научного исследования.
8. Технологическая фаза научного исследования.
9. Рефлексивная фаза научного исследования.
10. Методы математического планирования эксперимента.

Литература по разделу.

1. Пижурин А.,Пятков В. Методы и средства научных исследований. - М.: НИЦ ИНФРА-2015. – 264с.
2. Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. -2014. – 280 с.

Раздел 2. Организационно-правовые механизмы обеспечения информационной безопасности.

Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов.

Вопросы по разделу.

1. Информация как объект правового регулирования.
2. Законодательство РФ в области информационной безопасности.
3. Правовой режим защиты государственной тайны.
4. Правовые режимы защиты конфиденциальной информации.
5. Лицензирование и сертификация в информационной сфере.
6. Правовое регулирование оперативно-розыскных мероприятий в оперативно-розыскной и частной детективной и охранной деятельности.
7. Международное законодательство в области защиты информации.
8. Информационная безопасность и современные информационные технологии.
9. Организационные источники и каналы утечки информации.
10. Экономика информационной безопасности. Защита информации в экстремальных ситуациях.
11. Система организационной защиты информации.
12. Цели и задачи организационной защиты информации, ее связь с правовой защитой информации.
13. Средства и методы физической охраны объектов.
14. Порядок проведения аттестации объектов информатизации.
15. Организационные мероприятия по защите конфиденциальной информации.

Литература по разделу.

1. Федеральный закон Российской Федерации "Об информации, информатизации и защите информации" (№ 24-03 от 20.02.1995 г.).

2. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).

3. Березюк Л.П. Организационное обеспечение информационной безопасности: учеб. пособие/ Л. П. Березюк; ДВГУПС. Каф. "Информационные технологии и системы". - Хабаровск: Изд-во ДВГУПС, 2012. - 188 с.:

… Раздел 2. Организационно-правовые механизмы обеспечения информационной безопасности.

Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов.

Вопросы по разделу.

1. Информация как объект правового регулирования.
2. Законодательство РФ в области информационной безопасности.
3. Правовой режим защиты государственной тайны.
4. Правовые режимы защиты конфиденциальной информации.
5. Лицензирование и сертификация в информационной сфере.
6. Правовое регулирование оперативно-розыскных мероприятий в оперативно-розыскной и частной детективной и охранной деятельности.
7. Международное законодательство в области защиты информации.
8. Информационная безопасность и современные информационные технологии.
9. Организационные источники и каналы утечки информации.
10. Экономика информационной безопасности. Защита информации в экстремальных ситуациях.
11. Система организационной защиты информации.
12. Цели и задачи организационной защиты информации, ее связь с правовой защитой информации.
13. Средства и методы физической охраны объектов.
14. Порядок проведения аттестации объектов информатизации.
15. Организационные мероприятия по защите конфиденциальной информации.

Литература по разделу.

1. Федеральный закон Российской Федерации "Об информации, информатизации и защите информации" (№ 24-03 от 20.02.1995 г.).

2. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).

3. Березюк Л.П. Организационное обеспечение информационной безопасности: учеб. пособие/ Л. П. Березюк; ДВГУПС. Каф. "Информационные технологии и системы". - Хабаровск: Изд-во ДВГУПС, 2012. - 188 с.:

… Раздел 3. Теоретические основы компьютерной безопасности.

Архитектура электронных систем обработки данных; формальные модели; модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; стандарты по оценке защищенных систем; управление процессами функционирования систем защиты; парольные системы.

Вопросы по разделу.

1. Категории информационной безопасности.
2. Систематика методов и механизмов обеспечения компьютерной безопасности.
3. Понятие угроз безопасности, их классификация и идентификация
4. Политика безопасности. Субъектно-объектная модель компьютерной системы в процессах коллективного доступа к информационным ресурсам.
5. Монитор безопасности. Основные типы политик безопасности.
6. Общая характеристика моделей дискреционного доступа. Пятимерное пространство Хартсона.
7. Модели дискреционного доступа на основе матрицы доступа.

8. Модель распространения прав доступа Харрисона-Руззо-Ульмана (HRU).
9. Модель TAKE-GRANT.
10. Общая характеристика модели мандатного доступа.
11. Модель Белла-ЛаПадулы.
12. Понятие и общая характеристика скрытых каналов утечки информации.
13. Дискреционная модель Кларка-Вильсона.
14. Парольные системы. Выбор пароля. Требования к паролю. Количественные характеристики пароля.
15. Методология построения систем защиты информации в АС. Основные этапы разработки защищенных АС. Жизненный цикл АС. ГОСТ 34.601

5. Модель TAKE-GRANT.
6. Общая характеристика модели мандатного доступа.
7. Модель Белла-ЛаПадулы.
8. Понятие и общая характеристика скрытых каналов утечки информации.
9. Дискреционная модель Кларка-Вильсона.
10. Парольные системы. Выбор пароля. Требования к паролю. Количественные характеристики пароля.
11. Методология построения систем защиты информации в АС. Основные этапы разработки защищенных АС. Жизненный цикл АС. ГОСТ 34.601

Литература по разделу.

1. Грушо А.А. и др. Теоретические основы компьютерной безопасности. –М: Академия, 2011, - 271 с.
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: http://e.lanbook.com/view/book/5150/
3. Шестухина, В.И. Теоретические основы компьютерной безопасности: учеб.пособие / В.И. Шестухина. – Хабаровск: Изд-во ДВГУПС, 2012. – 174с.

Раздел 4. Безопасность систем баз данных.

Общие принципы построения баз данных: реляционная, иерархическая и сетевая модели; распределенные базы данных. Средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС. Журнализация, средства создания резервных копии и восстановления баз данных. Технологии удаленного доступа к системам баз данных. Аспекты информационной безопасности баз данных. Угрозы информационной безопасности баз данных. Политика безопасности. Контроль доступа к базе данных.

Вопросы по разделу.

1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных.
2. Критерии качества баз данных.
3. Сущность понятия безопасности баз данных.
4. Архитектура систем управления базами данных.
5. Источники угроз информации баз данных.
6. Классификация угроз информационной безопасности баз данных.
7. Угрозы, специфичные для систем управления базами данных.
8. Аутентификация и идентификация пользователей.
9. Методы дискреционного разграничения доступа.
10. Реализация мандатной модели доступа.
11. Обеспечение согласованности данных в многопользовательском режиме обработки.
12. Типы блокировок.
13. Аудит систем баз данных.
14. Концептуальное моделирование: недостатки реляционной модели данных для моделирования предметной области, определение концептуальной модели и способы представления.
15. Характеристики эффективной базы данных.

Литература по разделу.

1. Смирнов С.Н. Безопасность систем баз данных. Учебное пособие М. Гелиос 2011 г.- 352 с.
2. Гурвиц Г.А. Microsoft Access 2010. Разработка приложений на реальном примере. СПб.: БХВ-Петербург, 2010 – 496 с. – ил.

Раздел 5. Криптографические методы защиты информации.

История криптографии; характер криптографической деятельности; шифры и их свойства; композиции шифров; системы шифрования с открытыми ключами; виды информации, подлежащие закрытию, их модели и свойства; криптографическая стойкость шифров; модели шифров; основные требования к шифрам; совершенные шифры; теоретико-информационный подход к оценке криптостойкости шифров; вопросы практической стойкости; имитостойкость и помехоустойчивость шифров; принципы построения криптографических алгоритмов; криптографические хеш-функции; электронная цифровая подпись.

Вопросы по разделу.

1. Криптография. Основные термины и определения.
2. Классификация криптографических систем. Симметричные шифры.
3. Шифры замены. Шифры перестановки. Шифры гаммирования. Основные методы шифрования.
4. Схемы режима шифрования DES-ECB, DES-CBC, DES-CPB и DES-OFB.
5. Шифрование с открытым ключом. Основные понятия.
6. Алгоритм шифрования RSA.
7. Хэш-функции. Основные понятия и разновидности.
8. Криптографические протоколы. Протоколы обмена ключами.
9. Протоколы аутентификации. Разновидности и краткая характеристика.
10. Парольная идентификация/аутентификация.
11. Идентификация/аутентификация с помощью биометрических данных.
12. Электронная цифровая подпись. Общие сведения и разновидности.
13. Электронные платежи.
14. Основные сведения о криптоанализе и атаки на криптосистемы.
15. Компьютерная стеганография.

Литература по разделу.

1. Федеральный закон Российской Федерации "Об информации, информатизации и защите информации" (№ 24-03 от 20.02.1995 г.).
2. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).
3. Федеральный закон Российской Федерации "О персональных данных" (№ 152 от 27.07.2006 г.).
4. Федеральный закон Российской Федерации "Об электронной цифровой подписи" (№ 1-ФЗ от 26.12.2001 г.).
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2012 – 816 с. – ил.

Раздел 6. Обеспечение безопасности современных серверов баз данных.

Рекомендации по защите баз данных. Формирование защищенной среды. Предоставление разрешений через учетные записи служб. Защита файлов баз данных. Обеспечение безопасности сети. Шифрование данных на диске. Защищенная среда баз данных. Защита от инсайдерских атак.

Вопросы по разделу.

1. Обзор возможностей MS SQL Server 2014.
2. Серверы баз данных. Административные задачи управления сервером баз данных.
3. Архитектура вычислительной среды MS SQL Server, установка и настройка компонентов.
4. Основные задачи администрирования серверов баз данных. Объекты администрирования.
5. Структура базы данных в MS SQL Server. Системные и пользовательские таблицы. Назначение системных таблиц, хранимых процедур.

6. Архитектура информационной безопасности сервера баз данных. Режимы аутентификации в MS

SQL Server: проверка подлинности Windows, проверка средствами MS SQL Server, цифровые сертификаты.

7. Защита данных. Использование ролевой модели. Роли пользователей на уровне сервера баз данных. Инструменты управления ролями пользователей.

8. Создание и управление пользовательскими базами данных. Резервное копирование.

9. Пользователь и схема MS SQL Server. Встроенные пользователи.

10. Хранимые процедуры MS SQL Server. Пользовательские функции MS SQL Server.

12. Настройка MS SQL Server с помощью утилиты MS SQL Server Management Studio.

13. Субъекты безопасности. Роли пользователей на уровне базы данных. Инструменты управления ролями пользователей на уровне базы данных.

14. Средства мониторинга и анализа работы MS SQL Server. Журналы транзакций, их назначение.

15. Резервное копирование и восстановление данных. Модели восстановления данных MS SQL Server, их особенности.

Литература по разделу.

1. Бондарь А. Microsoft SQL Server 2014 в подлиннике. СПб.: БХВ-Петербург, 2014 – 592 с. – ил.
2. Dewson R. Beginning SQL Server for Developers. Apress, 2014 – 684 с. – ил.

Раздел 7. Обеспечение безопасности корпоративных систем.

Структура корпораций и предприятий; архитектура корпоративных ин-формационных систем. Создание концептуального плана защиты сетевой инфраструктуры. Проектирование логической инфраструктуры защиты сети. Проектирование физической инфраструктуры защиты сети. Проектирование безопасного управления сетью. Проектирование инфраструктуры обновления системы безопасности. Проектирование защиты межсетевого взаимодействия.

Вопросы по разделу.

1. Состав корпоративной информационной системы.
2. Бизнес-факторы, влияющие на проект защиты корпоративной информационной системы.
3. Проектирование защиты сети путем разбиения ее на сегменты.
4. Проектирование репликации Active Directory через брандмауэры.
5. Проектирование защиты данных внутри сети.
6. Источники угроз информации корпоративной системы.
7. Реализация принципа наименьших привилегий при обеспечении информационной безопасности.
8. Действия при проектировании безопасного администрирования.
9. Разработка стратегии аутентификации. Проектирование модели доверия для леса и домена.
10. Проектирование проверки подлинности в гетерогенной сети.

Литература по разделу.

1. Лецкий Э.К., Яковлев В.В. Корпоративные информационные системы на железнодорожном транспорте, 2014. — 256 с.
2. Хомоненко А.Д. и др. Модели информационных систем: учеб. пособие. 2015. — 188 с.
3. Корниенко А.А. Информационная безопасность и защита информации на железнодорожном транспорте. Ч.1. 2014. — 440 с.
4. Корниенко А.А. (под ред.). Информационная безопасность и защита информации на железнодорожном транспорте. Ч.2. 2014. — 448 с.

3. Оценка ответа обучающегося на контрольные вопросы, задания по практике.

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительн	Удовлетворитель	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам.	Значительные погрешности.	Незначительные погрешности.	Полное соответствие.

Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию.	Незначительное несоответствие критерию.	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер.
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.