МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Б2.В.04(Пд)
(индекс практики)

ПРОГРАММА ПРАКТИКИ

Производственная практика (преддипломная практика)
(наименование практики)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: 3 ЗЕ

Распределение часов практики по семестрам

Семестр	8	**Итого**
Форма контроля / **Вид занятий**	Зачет с оценкой	
Самостоятельная работа под руководством преподавателя	1,8	1,8
Промежуточная аттестация	0,2	0,2
Контактная работа	2	2
Иные формы	106	106
Итого	108	108

Программу практики составил(и):

Власов И.А.

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

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

Рецензирование программы практики:

☐ Отсутствует

☐ Рецензент

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

Программа практики составлена на основании ФГОС ВО и учебного плана направления подготовки 09.03.03 Прикладная информатика

Срок действия программы практики до «31» августа 2024 г.

УТВЕРЖДЕНО

На заседании ИИиЭБ

(протокол заседания № 2 от «сентября» 2022г.)

Производственная практика (преддипломная практика)

1.Цель практики

Цель – закрепление теоретических знаний, полученных студентами в процессе обучения в ВУЗе на основе практического применения их в практической деятельности, целенаправленного формирования профессиональных навыков, необходимых для последующего выполнения должностных обязанностей в области информационной безопасности.

2. Место практики в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная практика: «Мониторинг событий информационной безопасности», «Безопасность баз данных», «Безопасность веб-приложений», «Обеспечение безопасности критической информационной инфраструктуры», «Моделирование процессов и средств защиты информации».

Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее: Подготовка к сдаче и сдача государственного экзамена, Подготовка к процедуре защиты и процедура защиты ВКР.

3. Вид практики, способ и форма (формы) ее проведения

Вид практики: производственная практика (преддипломная практика).

Способ: -.

Форма проведения практики: дискретно

4. Тип практики
преддипломная практика

5. Место проведения практики
Промышленные предприятия г.о. Тольятти (отделы информационной безопасности).

6. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.8 Знает принципы сбора, отбора и обобщения информации	Знать: методику и технологию проведения информационного поиска, и критического анализа нормативных документов
		Уметь: анализировать информацию, применять системный подход для решения поставленных задач
		Владеть: навыками поиска и

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		критического анализа информации
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.13. Дает заключения о проведённых мероприятиях в порядке установленном законодательством РФ и регламентирующими документами ФСТЭК	Знать: Законодательство РФ и Нормативные документы регуляторов
		Уметь: Формулировать заключения по проведенным мероприятиям ИБ
		Владеть: Навыками разработки отчетных документов
	УК-2.14. Определяет круг задач в рамках поставленной цели для привлечения инвестиций в проект	Знать: Роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем
		Уметь: Применять основные методы управления информационной безопасностью организаций, объектов и систем
		Владеть: Практическими навыками в области стандартизации и нормотворчества в управлении информационной безопасностью
	УК-2.15. Решает профессиональные задачи информационной безопасности с применением программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования	Знать: Основные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ)
		Уметь: Применять программные средства системного, прикладного и специального назначения
		Владеть: Языками программирования для реализации задач ИБ
УК-3 Способен осуществлять социальное	УК-3.1 Определяет свою роль в команде для достижения	Знать: Должностные обязанности согласно задачам проекта

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
взаимодействие и реализовывать свою роль в команде	поставленной цели	Уметь: Реализовывать полученные теоретические знания на практике
		Владеть: Методами реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1. Грамотно и ясно строит диалогическую речь в рамках межличностного и межкультурного общения на государственном языке РФ	Знать: Грамотно и ясно строит диалогическую речь в рамках межличностного и межкультурного общения на государственном языке РФ и иностранном языке
		Уметь: Использует языковые формы и средства для достижения профессиональных целей на русском, родном и иностранном(ых) языке(ах).
		Владеть: Демонстрирует навыки находить, воспринимать и использовать информацию на иностранном языке, полученную из печатных и электронных источников для решения стандартных коммуникативных задач. Осуществляет выбор коммуникативных стратегий и тактик при ведении деловых переговоров
	УК-4.3 Демонстрирует способность понимать, анализировать и использовать средства иностранного языка для решения стандартных коммуникативных задач в общекультурном контексте	Знать: Грамотно и ясно строит диалогическую речь в рамках межличностного и межкультурного общения на государственном языке РФ и иностранном языке
		Уметь: Использует языковые формы и средства для достижения профессиональных целей на

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		русском, родном и иностранном(ых) языке(ах).
		Владеть: Демонстрирует навыки находить, воспринимать и использовать информацию на иностранном языке, полученную из печатных и электронных источников для решения стандартных коммуникативных задач.
УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1. Интерпретирует историю России, всеобщую историю в контексте мирового исторического развития	Знать: сущностную связь исторического развития мировых культур и цивилизаций
		Уметь: видеть прямую взаимосвязь и пути российского и мирового исторического развития в прошлом и настоящем
		Владеть: пониманием сущности многогранных отличий и уровней взаимосвязи исторического развития России и различных стран мира
	УК-5.2. Учитывает при социальном и профессиональном общении историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения	Знать: основные этапы и особенности исторического развития российской и мировой науки, техники, культуры
		Уметь: анализировать важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития
		Владеть: языком постановки историко-культурных вопросов применительно к областям межкультурных связей и коммуникаций
УК-6 Способен управлять своим временем, выстраивать и реализовывать	УК-6.1 Эффективно планирует собственное время	Знать: Направление саморазвития
		Уметь: Эффективно выстраивать

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
траекторию саморазвития на основе принципов образования в течение всей жизни		процесс саморазвития
		Владеть: Навыками управления своим временем
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1 Придерживается здорового образа жизни и определяет роль физической культуры в общекультурной и профессиональной подготовки	Знать: Методы физического воспитания для профессионально-личностного развития, физического самосовершенствования
		Уметь: Применять на практике знания методов физического воспитания для профессионально-личностного развития, физического самосовершенствования
		Владеть: Навыками здорового образа и стиля жизни с целью успешной 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-8.1. Использует методы и средства создания и поддержания безопасных условий жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении военных конфликтов	Знать: методы и средства создания и поддержания безопасных условий жизнедеятельности для сохранения природной среды
		Уметь: Применять методы и средства создания и поддержания безопасных условий жизнедеятельности для сохранения природной среды
		Владеть: Навыками обеспечения устойчивого развития общества, в том числе при угрозе и возникновении военных конфликтов
УК-9 Способен принимать обоснованные экономические решения в различных областях	УК-9.1 Знает базовые принципы функционирования экономики и экономического	Знать: Базовые принципы функционирования экономики и экономического развития
		Уметь:

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
жизнедеятельности	развития, цели и формы участия государства в экономике, методы личного экономического и финансового планирования, основные финансовые инструменты, используемые для управления личными финансами	Использовать финансовые инструменты для управления личным бюджетом, контролирует собственные экономические и финансовые риски
		Владеть: Навыками методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей
УК-10 Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 На основе знаний о праве и государстве, а также антикоррупционного и антитеррористического законодательства демонстрирует умения выявлять коррупционное поведение и имеет нетерпимое к нему отношение	Знать: Антикоррупционное и антитеррористическое законодательство
		Уметь: Выявлять коррупционное поведение и имеет нетерпимое к нему отношение
		Владеть: Навыками выявления коррупционного поведения
ПК-1 Способен осуществлять оптимизацию управления жизненным циклом распределенных данных с учетом информационной безопасности	ПК-1.4 Демонстрирует понимание работы реляционной модели данных и принципов защиты информации при ее построении и эксплуатации	Знать: -технические каналы утечки информации - реляционную модель данных СЗИ
		Уметь: - получать информацию от сетевых сервисов
		Владеть: -методами количественного анализа процессов обработки, поиска и передачи информации
ПК-2 Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой,	ПК-2.4 Разрабатывает обоснование и выбор рационального решения по уровню обеспечения защищенности инфокоммуникационной системы с учетом	Знать: - методику оценки уровня защищенности
		Уметь: - разработать обоснование решения по уровню обеспечения защищенности ИС

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
современных операционных систем и сетевых оболочек в профессиональной деятельности	заданных требований	Владеть: - навыками разработки ОРД
ПК-3 Способен оценивать угрозы безопасности информации операционных систем и сетей	ПК-3.1 Использует принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	Знать: - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
		Уметь: - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
		Владеть: - навыками оценки угроз безопасности сетевой инфраструктуры
	ПК-3.6 Демонстрирует владение навыками эффективного использования программно-аппаратные средства обеспечения информационной безопасности	Знать:
		Уметь:
		Владеть:
ПК-4 Способен применять знания фундаментальной и прикладной математики в разработке программного обеспечения	ПК-4.1 Использует математический аппарат аналитической геометрии и высшей алгебры при решении профессиональных задач	Знать: Математический аппарат аналитической геометрии и высшей алгебры при решении профессиональных задач
		Уметь: Применять математический аппарат аналитической геометрии и высшей алгебры при решении профессиональных задач
		Владеть: Математическим аппаратом при решении физических задач.

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-5 Способен осуществлять выбор языка программирования и моделировать решение для реализации программного обеспечения	ПК-5.1. Знает технологии моделирования ПО.	Знать: технологии создания программных решений на современных языках программирования. Уметь: формализовать постановку прикладных задач исследования с целью программирования решения. Владеть: навыками использования интегрированных сред разработки для создания программ.
ПК-6 Способен производить оценку эффективности применения программно-аппаратных средств защиты информации, осуществлять мониторинг функционирования программно-аппаратных средств защиты информации	ПК-6.1 Применяет методику, средства и инструменты для проведения мониторинга	Знать: - способы и средства защиты информации от утечек по техническим каналам - средства и инструменты анализа защищенности
		Уметь: - измерять физические параметры сигнала и определять комплекс мер по защите сигнала от утечек - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.
		Владеть: - навыками работы с программно-аппаратными комплексами защиты информации по техническим каналам
ПК-7 Способен разрабатывать и внедрять организационные меры по защите информации на основе руководящих и методических документов уполномоченных федеральных органов	ПК-7.4 Демонстрирует умение в организации работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну,	Знать: -Актуальные требования регуляторов в вопросах обработки и защиты персональных данных; - Нормативно-правовое обеспечение вопросов обработки и защиты персональных данных в организации

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
исполнительной власти по защите информации	и конфиденциальной информации)	Уметь: Разрабатывать необходимую организационно-распорядительную документацию согласно требований законодательства в трактовке регуляторов
		Владеть: Навыками подготовки пользователей информационных систем работе с персональными данными, и навыками обеспечения целостности цифровых доказательств
	ПК-7.5 Демонстрирует навыки организации работы коллектива исполнителей, определение порядка выполнения работ по осуществлению правового, организационного и технического обеспечения защиты информации	Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
		Уметь: применять криптографические алгоритмы и протоколы для решения задач обеспечения аутентификации и защиты информации в информационных системах Владеть: навыками применения криптографических алгоритмов
ПК-8 Способен составлять технико-экономическое обоснование проектных решений и техническое задание на разработку программного обеспечения	ПК - 8.6 Демонстрирует умение выстраивать процесс управления ИБ на основе риск - ориентированного подхода.	Знать: - принципы и требования разработки безопасного ПО - модели представления системы информационной безопасности
		Уметь: - встроить в процесс управления ИБ мониторинг безопасной разработки
		Владеть: - -методами оценки инвестиций в информационную безопасность
	ПК-8.5 Демонстрирует навыки построения как отдельных процессов	Знать: принципы построения и развития социальной

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
	управления ИБ, так и системы процессов в целом.	инженерии, основы теории системного подхода при решении задач защиты информации
		Уметь: провести оценку проблемной ситуации в сфере социальной инженерии, выявить основные закономерности и тенденции применения форм и методов нарушителями
		Владеть: Владеет основами социнженерии, методами работы нарушителей с целью их выявления и нейтрализации
ПК-9 Способен формулировать политики информационной безопасности	ПК-9.7 Демонстрирует умение разрабатывать ОРД	Знать: - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
		Уметь: - разрабатывать и пользоваться нормативными документами по защите информации - разрабатывать политику безопасности
		Владеть: - навыками разработки ОРД на основе определения границ безопасности инфраструктуры
ПК-10 Способен осуществлять моделирование решений по реализации программного обеспечения и управлению БД	ПК-10.1 Использует знания стандартов ИБ и НПА	Знать: - роль стандартов и спецификаций; - основные понятия и идеи, изложенные в стандартах в области информационной безопасности
		Уметь: - применять основные требования международных и российских нормативных правовых актов в области обеспечения информационной

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		безопасности - использовать утвержденные в нормативных правовых актах и методических документах формы документации
		Владеть: - основами ИБ: - навыками работы с нормативными правовыми актами
	ПК-10.4 Использует принципы организации комплексной безопасности	Знать: - способы решения при возникновении проблемы, чрезвычайных ситуаций и военных конфликтов - современные подходы к управлению КБ и направления их развития; - принципы построения КБ; принципы разработки процессов управления КБ; - взаимосвязи отдельных процессов управления КБ;
		Уметь: - создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды - определять цели и задачи, решаемые разрабатываемыми процессами управления КБ
		Владеть: - способностью создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
	ПК-10.10 Использует знания математического и имитационное моделирования систем защиты информации	Знать: - математическое и имитационное моделирование систем защиты информации
		Уметь: - применять модели процессов в информационном обмене в системах защиты информации, модели процессов сохранения конфиденциальности информации
		Владеть: - алгоритмами создания системы комплексной защиты, методологией разработки моделей, инструментарием имитационного моделирования
	ПК-10.11 Умеет применять модели процессов в информационном обмене в системах защиты информации	Знает: Математическое и имитационное моделирование систем защиты информации
		Умеет: - разрабатывать модели управления рисками информационной безопасности
		Владеет: - навыками построения имитационной модели
	ПК-10.12 Владеет алгоритмами создания системы комплексной защиты, методологией разработки моделей	Знает: - алгоритм создания системы комплексной защиты, методологию разработки моделей
		Умеет: - разрабатывать ролевую матрицу доступа
		Владеет: - инструментарием имитационного моделирования
ПК-11 Способен противодействовать	ПК-11.1 Использует знания основ	Знать: - основы современные

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
угрозам безопасности информации с использованием средств защиты информации операционных систем и сетей, включая средства криптографической защиты информации	современных криптографических алгоритмов и протоколы для обеспечения информационной безопасности	криптографические алгоритмы и протоколы для обеспечения информационной безопасности; - нормативно-правовые акты по КЗИ
		Уметь: - применять криптографические алгоритмы и протоколы для решения задач обеспечения аутентификации и защиты информации в информационных системах
		Владеть: - навыками работы с программными и аппаратными средствами защиты информации в компьютерных системах; - навыками разработки РПД по КЗИ.
	ПК-11.4 Использует знания методов и средств контроля технической защиты информации	Знать: возможности технических разведок; методы и средства контроля технической защиты информации
		Уметь: - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации
		Владеть: - основами поиска закладных устройств утечки информации; - методиками проверки защищённости объектов информатизации на соответствие требованиям нормативных документов
	ПК-11.9 Владеет навыками навыками поиска и нейтрализации	Знать: - уязвимости, присутствующие в ОС и ПО;

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
	вредоносного ПО	- способы борьбы с вредоносным ПО и уязвимостями
		Уметь: - обнаруживать присутствие вредоносного программного кода в статическом и динамическом режимах
		Владеть - навыками поиска и нейтрализации вредоносного ПО

7. Структура и содержание практики

Вид учебной работы	Этапы практики	Семестр	Объем, ч.	Баллы	Формы текущего контроля (наименование оценочного средства)
ИФ	Ознакомление с нормативной документацией ТГУ	8	2	-	-
ИФ	Ознакомление со сроками прохождения практики	8	1	-	-
ИФ	Практическое задание 1 Подписанный со стороны профильной организации договор по практике	8	2	10	Подписанный со стороны профильной организации договор по практике
ИФ	Ознакомление с общим рабочим графиком (планом) проведения практики	8	1	-	-
ИФ	Практическое задание 2 Индивидуальный график (план) проведения практики	8	1	5	Индивидуальный график (план) проведения практики
ИФ	Практическое задание 3 Программно-аппаратные методы и средства защиты информации, применяемые на предприятии	8	10,16	15	Список используемой литературы и используемых источников
ИФ	Практическое задание 4 Оценка защищенности сети передачи данных	8	70	20	Графическая часть
ИФ	Практическое задание 5 Оформление отчета по практике Отчет по практике	8	19,84	50	Отчет по практике
СРП	Консультации с руководителем практики	8	1,8	-	-
ПА	Сдача зачета (с оценкой)	8	0,2		Вопросы к зачету
Форма (формы) отчетности по практике					Отчет по практике
		Итого:	**108**	**100**	

8. Образовательные технологии

Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Самостоятельная работа. Индивидуальное задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

9. Методические указания

Прохождение практики подразумевает выполнение практических заданий:

- Ознакомление с нормативной документацией ТГУ
- Ознакомление со сроками прохождения практики
- Практическое задание 1. При выполнении данного задания обучающиеся оформляют договор с организацией на прохождение практики. Итогом выполнения этого задания является - Подписанный со стороны профильной организации договор по практике.
- Ознакомление с общим рабочим графиком (планом) проведения практики
- Практическое задание 2. При выполнении данного задания обучающиеся составляют по программе практики индивидуальный график проведения практики. С указанием сроков выполнения всех заданий. Итогом выполнения данного задания является - Индивидуальный график (план) проведения практики.

– Практическое задание 3. Программно-аппаратные методы и средства защиты информации, применяемые на предприятии

Практическое задание 4. Оценка защищенности сети передачи данных

– Практическое задание 5. Оформление отчета по практике.

10. Оценочные средства

10.1. Паспорт оценочных средств

Код контролируемой компетенции (или ее части)	Наименование оценочного средства
УК-1; УК-2; УК-3; УК-4; УК-5;УК-6; УК-7; УК-8; УК-9; УК-10; УК-11; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8	*Вопросы к зачету с оценкой № 1-60.* *Отчет по практике*

10.2. Типовые задания или иные материалы, необходимые для текущего контроля успеваемости

10.2.1. Договор по практике

_____

(наименование оценочного средства)

Типовой(ые) пример(ы) задания(ий)

Поиск профильной организации, заключение договора, загрузка договора в курс.

Краткое описание и регламент выполнения

Учащийся оформляет договор по практике.

Загружает в систему Росдистант.

Критерии оценки:

Наличие договора в контенте – задание выполнено.

Отсутствие договора в контенте – задание не выполнено.

10.2.2. Индивидуальный график проведения практики

Типовой(ые) пример(ы) задания(ий)

Составление и согласование индивидуального графика (плана) проведения практики

Краткое описание и регламент выполнения

Учащийся составляет индивидуальный график проведения практики

Учащийся согласовывает индивидуальный график проведения практики с руководителем по практике и представителем от профильной организации.

Учащийся загружает индивидуальный график в контент.

Критерии оценки:

Наличие индивидуального графика (плана) проведения практики в контенте – задание выполнено.

Отсутствие индивидуального графика (плана) проведения практики в контенте – задание не выполнено.

10.2.3. Программно-аппаратные методы и средства защиты информации, применяемые на предприятии

Типовой(ые) пример(ы) задания(ий)

Программно-аппаратные методы и средства защиты информации, применяемые на предприятии

Краткое описание и регламент выполнения

Обучающийся анализирует состав программно-аппаратных методов и средств защиты информации, применяемых в инфраструктуре предприятия и описывает характеристики, назначение и метод использования отдельно для группы аппаратных средств и программных.

Отдельно описать применяемые на предприятии:

- криптографические методы и средства защиты информации
- методы и средства инженерно-технической защиты информации

Критерии оценки:

Наличие задания по практике в контенте – задание выполнено.

Отсутствие задания по практике в контенте – задание не выполнено.

10.2.4. Оценка защищенности сети передачи данных

Типовой(ые) пример(ы) задания(ий)

Оценка защищенности сети передачи данных

Краткое описание и регламент выполнения

Обучающийся рассматривает формальную модель системы защиты сети передачи данных, выводит качественные оценки уровня защищенности сети путем сопоставления свойств и параметров сети с многократно опробованными на практике и стандартизированными критериями оценки защищенности. Проводит анализ защищенности по типовой методике.

В отчете указывает исходные данные по обследуемой сети, применяемы методы оценки, инструментарий и выводы по результатам оценки защищенности.

Критерии оценки:

Наличие графической части в контенте – задание выполнено.

Отсутствие графической части в контенте – задание не выполнено.

10.2.5. Подготовка и загрузка отчета по практике

Типовой(ые) пример(ы) задания(ий)

Составление отчета по практике.

Краткое описание и регламент выполнения

Разделы, подразделы отчета определяются с руководителем отчета, исходя из поставленной цели, задач и методов достижения целей и задач. Обучающийся должен продемонстрировать владение нормативной правовой документацией, анализом данных, формулированием выводов по результатам анализа, методами и способами решения задач, методами представления данных (диаграммы, блок-схемы, таблицы, графики, процедуры и т.д.).

Критерии оценки:

Наличие отчета по практике в контенте – задание выполнено.
Отсутствие отчета по практике в контенте – задание не выполнено.

10.3. Оценочные средства для промежуточной аттестации

10.3.1. Вопросы к промежуточной аттестации

№ п/п	Вопросы к зачету с оценкой
1.	Назовите причины информационных угроз
2.	Какие личностно-профессиональные характеристики сотрудников способствуют реализации угроз ИБ
3.	Какие вы знаете компьютерные преступления?
4.	Какие элементы информационной инфраструктуры Вы знаете?
5.	Что понимается под угрозой безопасности информации?
6.	Назовите объекты информационной безопасности на предприятии
7.	Дайте характеристику Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
8.	Назовите основные принципы политики безопасности
9	Что включает политика безопасности верхнего уровня?
10	Что включает политика управления паролями?
11	На каких принципах базируется системный подход к защите информации?
12	Что такое электронная подпись и для чего она используется?
13	Что входит в состав организационно-технических мер по защите информации?
14	Какие качества проверяются у лиц при приеме на работу в сфере ИБ?
15	Для чего применяют межсетевые экраны?
16	Назовите меры по защите информации в интернете
17	Назовите основные источники проникновения вирусов
18	В чем разница симметричного и ассиметричного шифрования?
19	Какие особенности компании необходимо учитывать при разработке системы защиты?
20	Что необходимо защищать в корпоративной сети?
21	Что включает план DPR?
22	Как оценить эффективность инвестиций в информационную безопасность?
23	Что такое фишинг?
24	Перечислите виды ответственности за использование не лицензионного программного обеспечения?
25	Что в криптографии называют «ключом»?
26	Приведите примеры шифров с открытым ключом
27	В отношении каких сведений установлен режим защиты информации?
28	Проведите классификацию мер защиты информации
29	Охарактеризуйте организационные меры защиты информации
30	Охарактеризуйте технические меры защиты информации
31	Охарактеризуйте правовые меры защиты информации
32	Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных компьютерных программ?
33	Какие существуют проблемы построения защищенных информационных систем? Опишите эти проблемы
34	Что необходимо сделать для защиты информационных ресурсов от

	несанкционированного доступа ?
35	Дайте характеристику целям и задачам защиты информации
36	Контроль доступа к веб-приложению. Ограничения прав системных учётных записей, привести практические примеры.
37	Методы аутентификации в приложении. Способы двухфакторной аутентификации
38	Примеры мер защиты от внедрения вредоносного кода
39	Этапы проведения атаки на веб приложение
40	Этапы проверки безопасности сайта
41	Перечислить методы обнаружения вредоносных программ
42	Принципы этичного хакинга. Последствия их нарушений
43	Какие виды целостности поддерживаются в реляционной БД?
44	Что такое о ссылочная целостность?
45	Привести примеры нарушения работы БД, связанные с ссылочной целостностью
46	Порядок индексации БД
47	К чему приводит удаление индексов?
48	Что такое системная привилегия СУБД?
49	Назовите системные привилегии для таблиц
50	Что такое дискреционное разграничение доступа?
51	Как использовать журналы логирования?
52	Как организуется защита подключений?
53	Перечислить базовый состав мер по контролю сетевого трафика
54	Какие проблемы выявляются при тестировании на проникновение?
55	Как осуществляется пассивный перехват сетевого трафика?
56	Какими способами можно осуществить мониторинг сетевых подключений?
57	Как осуществляется активный перехват сетевого трафика?
58	Перечислить основные причины уязвимостей
59	Каковы этапы создания и функционирования СОИБ ЗОКИИ
60	С кем нужно согласовывать Перечень объектов КИИ, подлежащих категорированию?

Форма проведения промежуточной аттестации	**Критерии и нормы оценки**	
зачет с оценкой (по накопительному рейтингу)	«отлично»	85-100 баллов
	«хорошо»	70-84 баллов
	«удовлетворительно»	55-69 баллов
	«неудовлетворительно»	0-54 баллов

11. Учебно-методическое и информационное обеспечение практики

11.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1.	Нестеров С.А.	Основы информационной безопасности	учебное пособие	2022г.	https://e.lanbook.com/books/1545
2.	Прохорова О.В.	Информационная безопасность и защита информации	учебное пособие	2022г.	https://e.lanbook.com/book/217445?category=1545
3.	Никифоров С.Н.	Методы защиты информации. Защищенные сети	учебное пособие	2021 г	https://e.lanbook.com/book/171868?category=1545
4.	Раков А.С., Маслов О.Н., Губарева О.Ю., Почепцов А.О., Гуреев В.О.	Техническая защита информации: учебное пособие	учебное пособие	2020	эбс-Лань
5.	Петренко В.И.	Защита персональных данных в информационных системах	Практикум	2022	https://reader.lanbook.com/book/264242
6.	Н.В. Скабцов	Аудит безопасности информационных систем	учебно-методическое пособие	2020	эбс-Лань
7	Никифоров С. Н.	Методы защиты информации. Защита от внешних вторжений	Учебное пособие	2022	эбс-Лань

11.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1.	А. И. Бирюков	Информационная безопасность: защита и нападение 2-е изд.)	учебно-методическое пособие	2019г.	эбс-Лань
2.	А.В. Моргунов	Информационная безопасность:	учебно-методическое пособие	2019г.	https://e.lanbook.com/book/152227?category=1545
3.	Рагозин Ю. Н.	Инженерно-техническая защита информации: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности	учебное пособие	2019	эбс-Лань

11.3. Перечень профессиональных баз данных и информационных справочных систем

- Нормативные правовые документы. [Электронный ресурс] Режим доступа: http://www.consultant.ru
- Документы ФСТЭК [Электронный ресурс] Режим доступа: http://www.fstec.ru/
- Электронная библиотечная система IPRbooks. [Электронный ресурс] Режим доступа: http://www.iprbookshop.ru/
- Научная электронная библиотека [Электронный ресурс] Режим доступа: http://elibrary.ru/defaultx.asp?
- Энциклопедия информационной безопасности. [Электронный ресурс] Режим доступа: https://securelist.ru/enciklopediya
- Набор технологий и программ для работы в сети [Электронный ресурс] Режим доступа: http://internetsecure.ru/
- Информационно-аналитический портал по безопасности [Электронный ресурс] Режим доступа: http://www.anti-malware.ru/
- Национальный форум информационной безопасности [Электронный ресурс] Режим доступа: http://www.infoforum.ru/
- Журнал «Защита информации. Инсайд» [Электронный ресурс] Режим доступа: http://www.inside-zi.ru
- Портал «InformationSecurity» [Электронный ресурс] Режим доступа: http://www.itsec.ru
- Журнал «Безопасность информационных технологий» [Электронный ресурс] Режим доступа: https://bit.spels.ru/index.php/bit/index
- Библиотека ИБ – эксперта [Электронный ресурс] Режим доступа: https://securitymedia.org/info/biblioteka-ib-eksperta.html
- Банк угроз ФСТЭК [Электронный ресурс] Режим доступа: https://bdu.fstec.ru/threat-section/negatives
- Форум Античат [Электронный ресурс] Режим доступа: https://forum.antichat.com
- Справочно-правовая система по законодательству Российской Федерации [Электронный ресурс]. Режим доступа: http://www.garant.ru
- Информационно-правовая система по законодательству Российской Федерации [Электронный ресурс]. Режим доступа: http://www.kodeks.ru
- WebofScience [Электронный ресурс]: мультидисциплинарная реферативная база данных. – Philadelphia: ClarivateAnalitics, 2016–. – Режим доступа: apps.webofknowledge.com. – Загл. с экрана. – Яз. рус., англ.
- Scopus [Электронный ресурс]: реферативная база данных. – Netherlands: Elsevier, 2004–. – Режим доступа: scopus.com. – Загл. с экрана. – Яз. рус., англ.
- Elibrary [Электронный ресурс]: научная электронная библиотека. – Москва: НЭБ, 2000–. – Режим доступа: elibrary.ru. – Загл. с экрана. – Яз. рус., англ.
- SpringerLink [Электронный ресурс]: [база данных]. – Switzerland: SpringerNature, 1842–. – Режим доступа: link.springer.com. – Загл. с экрана. – Яз. англ.
- ScienceDirect [Электронный ресурс]: коллекция электронных книг издательства Elsevier. – Netherlands: Elsevier, 2018–. – Режим доступа: sciencedirect.com. – Загл. с экрана. – Яз. англ.
- Cambridgeuniversitypress [Электронный ресурс]: журналы издательства. – Cambridge: Cambridgeuniversitypress, 2018–. – Режим доступа: cambridge.org. – Загл. с экрана. – Яз. англ.

NEICON [Электронный ресурс]: электронная информация: архив научных журналов. – Москва: НЭИКОН, 2002–. – Режим доступа: neicon.ru/resources/archive. – Загл. с экрана. – Яз. рус., англ.

11.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	Office Standart	- OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3	Консультант+	- Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

11.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по практике

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф