ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Б2.О.02(П) ПРОИЗВОДСТВЕННАЯ ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

1. АННОТАЦИЯ

1.1 Производственная технологическая практика (далее по тексту – практика) входит в состав практики основной профессиональной образовательной программы высшего образования (далее по тексту ОПОП ВО) и учебного плана подготовки бакалавров по направлению подготовки/специальности 10.03.01 Информационная безопасность профилю подготовки/специализации Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности).

1.2 Практика проходит в 2 курсе(ах) в 4 семестре(ах). и состоит из:

1. Запись в дневникепрактики

2. Запись в дневникепрактики

3. Выполнение определённых видов деятельности в рамках практики, осуществляемой на предприятии

2. Вид и тип практики, способы и формы ее проведения

2.1 Тип практики: .

Основными целями практики являются:

- подготовка к решению производственных задач предприятия, сбор материала для выполнения выпускной квалификационной работы;
- закрепление и углубление теоретических знаний, полученных при изучении дисциплин

учебного плана;

- приобретение и развитие необходимых практических умений и навыков в соответствии

с требованиями к уровню подготовки выпускника;

- изучение современного состояния и направлений развития компьютерной техники и информационных технологий;
- изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем информационной безопасности;
- изучение комплексного применения методов и средств обеспечения информационной

безопасности;

- изучение источников информации и системы оценок эффективности ее использования;
- закрепление и углубление практических навыков в области информационной безопасности;
- повышение уровня освоения компетенций в профессиональной деятельности

2.2 Способы проведения практики: выездная.

Стационарная практика проводится в образовательной организации или ее филиале, в котором обучающиеся осваивают образовательную программу, или в иных организациях, расположенных на территории населенного пункта, в котором расположена образовательная организация или филиал. Выездная практика проводится в том случае, если место ее проведения расположено вне населенного пункта, в котором расположена образовательная организация или филиал. Выездная практика может проводится в полевой форме в случае необходимости создания специальных условий для ее проведения.

2.3 Формы проведения практики: непрерывно – путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения всех видов практик, предусмотренных образовательной программой

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

3.1 Взаимосвязь планируемых результатов обучения при прохождении практики (знания, умения, навыки и (или) опыт деятельности) и планируемых результатов освоения образовательной программы (компетенций обучающегося) представлена в таблице 1 .

Таблица 1. Взаимосвязь планируемых результатов обучения при прохождении практики и планируемых результатов освоения образовательной программы

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1 Разрабатывает и реализовывает политики управления доступом в компьютерных системах	*Знать:* источники угроз безопасности информации *Уметь:* применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации *Владеть:* навыками сопровождения и управления системами защиты информации

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.2 Обеспечивает защиту информации при работе с базами данных, при передаче по компьютерным сетям	*Знать:* структуру политики безопасности и основные законодательно-правовые положения защиты информации, виды и состав угроз информационной безопасности и меры из предотвращения *Уметь:* классифицировать угрозы информационной безопасности применительно к объектам защиты *Владеть:* навыками анализировать состояние информационной безопасности на конкретном объекте защиты, практическими навыками в использовании основных методов и средств обеспечения информационной безопасности
	ОПК-1.3 Оценивает уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	*Знать:* технологии хранения, поиска и сортировки информации *Уметь:* использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности *Владеть:* приемами поиска, систематизации, хранения и обработки информации

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1 Проводит анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	*Знать:* принципы организации информационных систем в соответствии с требованиями по защите информации *Уметь:* анализировать и оценивать угрозы информационной безопасности обьекта *Владеть:* методами и средствами выявления угроз безопасности
	ОПК-2.2 Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям	*Знать:* структуру организации и управления деятельностью подразделений по защите объектов информатизации *Уметь:* проводить информационную характеристику и организационную структуру объектов информатизации предприятия *Владеть:* навыками выработки предложений о возможности внедрения дополнительных мер, в том числе, для обеспечения информационной безопасности функционирования информационных систем предприятия при взаимодействии с внешними информационными сетями
	ОПК-2.3 Разрабатывает , внедряет и сопровождает комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	*Знать:* цели, задачи, принципы и основные направления обеспечения информационной безопасности *Уметь:* анализировать качество средств и методов защиты информационных систем *Владеть:* навыками формальной постановки и решения задачи обеспечения информационной безопасности

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.4 Проводит аудит защищенности объекта информатизации в соответствии с нормативными документами	*Знать:* методику проведения аудита информационной безопасности информационных систем и объектов информатизации *Уметь:* оценивать эффективность и надежность защиты систем и объектов информатизации *Владеть:* методами анализа и оценки механизмов защиты систем и объектов информатизации
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.1 Применяет математические модели и решать задачи помехоустойчивого кодирования при проектировании защищенных автоматизированных систем	*Знать:* основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации *Уметь:* исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач *Владеть:* навыками использования справочных материалов по математическому анализу, использования расчетных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.2 Применяет технологии защиты информации при создании защищенных автоматизированных систем	*Знать:* классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщенную структуру операционных систем; назначение и основные компоненты систем баз данных *Уметь:* применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет *Владеть:* навыками поиска информации в глобальной информационной сети Интернет; применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.3 Осуществляет эксплуатацию и проводить техническое обслуживание защищенных автоматизированных систем	*Знать:* принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации *Уметь:* обеспечивать работоспособность, обнаруживать и устранять неисправности *Владеть:* навыками диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления
	ОПК-5.4 Проводит мониторинг функционирования защищенных автоматизированных систем	*Знать:* состав и принципы работы автоматизированных систем, операционных систем и сред *Уметь:* осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем *Владеть:* навыками эксплуатации компонентов систем защиты информации автоматизированных систем

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 Использует нормативные правовые акты в профессиональной деятельности	*Знать:* основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации *Уметь:* обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав *Владеть:* навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.2 Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	*Знать:* нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации *Уметь:* разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации *Владеть:* навыками по разработке политики безопасности объекта информатизации
	ОПК-6.3 Организовывает технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами	*Знать:* методы пресечения разглашения конфиденциальной информации *Уметь:* применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации *Владеть:* навыками сопровождения и управления системами защиты информации

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	*Знать:* основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы *Уметь:* применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы *Владеть:* навыками составления технической документации на различных этапах жизненного цикла информационной системы

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.2 Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*Знать:* сущность и значение информации в развитии современного общества *Уметь:* на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности решать стандартные задачи *Владеть:* методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.3 Проводит решение стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*Знать:* используемы е в современной экономике методы информационно-коммуникационных технологий для решения задач информационной безопасности *Уметь:* использовать базовые знания об информационных системах для решения исследовательских профессиональных задач *Владеть:* навыками разработки специализированных программ для решения задач профессиональной сферы деятельности
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Применяет математические модели и решать задачи криптографического преобразования при решении задач защиты информации	*Знать:* Математические модели, методы и алгоритмы решения типовых задач *Уметь:* строить алгоритмы решения типовых задач анализа информации *Владеть:* навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.2 Определяет и анализирует технические каналы утечки информации	*Знать:* принципы работы с системами предотвращения утечек *Уметь:* изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации *Владеть:* навыками расчета контролируемой зоны, в пределах которой могут происходить утечки информации
	ОПК-9.3 Проводит работы по установке и настройке средств технической защиты информации	*Знать:* технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении *Уметь:* проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией *Владеть:* навыками работы по установке и настройке средств технической защиты информации

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 Способен организовывать и поддерживать выполнение комплекса мер по информационной безопасности	*Знать:* программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях *Уметь:* конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности *Владеть:* принципами формирования политики информационной безопасности объекта информатизации
	ОПК-10.2 Способен проводить построения как отдельных процессов управления информационной безопасностью, так и системы процессов в целом	*Знать:* стандартные вероятностно-статистические методы анализа экспериментальных данных *Уметь:* строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных *Владеть:* навыками по проведению эксперимента по заданной методике с составлением итогового документа

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.3 Используя современные методы и средства разрабатывает процессы управления информационной безопасности, учитывающие особенности функционирования и решаемых задач, и оценивает их эффективность	*Знать:* способы поиска и обработки информации, методы работы с научной информацией *Уметь:* обобщать, анализировать и систематизировать научную информацию в области информационной безопасности *Владеть:* навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов;	ОПК-11.1 Проводит испытания по оценки защищенности объектов информатизации на основе существующих методик ФСТЭК	*Знать:* стандартные вероятностно-статистические методы анализа экспериментальных данных *Уметь:* строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных *Владеть:* навыками по проведению эксперимента по заданной методике с составлением итогового документа

ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов;	ОПК-11.2 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	*Знать:* основные понятия и методы математической статистики *Уметь:* логически мыслить, подбирать формулы, соответствующие типам задач *Владеть:* основными приемами и способами вычисления вероятностей наступления случайных событий, их числовых характеристик, оценок
	ОПК-11.3 Принимает участие в проведении экспериментальных исследований системы защиты информации.	*Знать:* основные понятия *Уметь:* логически мыслить, подбирать формулы, соответствующие типам задач *Владеть:* навыками использования математических моделей теории вероятностей и математической статистики

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1 Проводит сбор исходных данных на объекте информатизации	*Знать:* принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта *Уметь:* определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации *Владеть:* навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений
	ОПК-12.2 Осуществляет обработку и оценку исходных данных	*Знать:* основные виды и процедуры обработки информации, модели и методы решения задач обработки информации *Уметь:* осуществлять выбор модели и средства построения информационной системы и программных средств *Владеть:* навыками обеспечения сбора данных для анализа использования и функционирования информационной системы

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.3 Разрабатывает технико-экономическое обоснование проектных решений	*Знать:* основы проведения технико-экономического обоснования *Уметь:* прогнозировать технико-экономические показатели *Владеть:* практическими навыками и умениями проведения технико-экономического анализа
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	ОПК-4.1.1 Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации	*Знать:* основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты *Уметь:* использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации *Владеть:* навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности

ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	ОПК-4.1.2 Обеспечивает блокирование возможных каналов утечки информации через технические средства с помощью специальных устройств	*Знать:* структуру государственной системы защиты информации от утечки по техническим каналам *Уметь:* изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации *Владеть:* расчетом контролируемой зоны, в пределах которой могут происходить утечки информации
	ОПК-4.1.3 Осуществляет подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности в автоматизированных системах	*Знать:* принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией *Уметь:* обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно-справочными системами *Владеть:* навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы, нормативных и методических документов

ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	ОПК-4.3.1 Способен применять основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак	*Знать:* основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак *Уметь:* определять рациональные меры для выбора необходимых средств защиты информации и уметь их оценивать *Владеть:* методами защиты информации в операционных системах и в пользовательских приложениях
	ОПК-4.3.2 Выявляет принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях	*Знать:* основные принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях *Уметь:* выявлять слабости защиты ОС, ВС и СУБД и использовать их для вскрытия защиты *Владеть:* навыками анализа и администрирования подсистем защиты современных ОС, ВС и СУБД

ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	ОПК-4.3.3 Способен использовать сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации (в том числе криптографических)	*Знать:* сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации *Уметь:* применять и администрировать средства программно-аппаратной защиты информации *Владеть:* навыками использования межсетевых экранов и систем обнаружения вторжений
	ОПК-4.3.4 Выявляет средства и методы защиты от НСД хранимой информации с использованием возможностей устройств	*Знать:* средства и методы защиты от НСД хранимой информации с использованием возможностей устройств записи и чтения *Уметь:* планировать программно-аппаратную подсистему политики безопасности организации *Владеть:* методами защиты компьютерной информации от НСД

ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем;	ОПК-4.4.1 Способен диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции систем защиты автоматизированных систем	*Знать:* методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации *Уметь:* диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации *Владеть:* навыками тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации
	ОПК-4.4.2 Способен осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации	*Знать:* особенности и способы применения программных и программно-аппаратных средств защиты информации *Уметь:* устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации *Владеть:* навыками использования программных и программно-аппаратных средств для защиты информации в сети

ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем;	ОПК-4.4.3 Применяет типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	*Знать:* номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации *Уметь:* применять инженерно-технические средства физической защиты объектов информатизации *Владеть:* навыки выявлении технических каналов утечки информации

4. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

Требования к предшествующим знаниям представлены в таблице 2. Перечень дисциплин, для которых практика «Производственная технологическая практика» является основополагающей, представлен в табл. 3.

Таблица 2. – Требования к пререквизитам практики

Компетенция	Дисциплина/Практика
ОПК-1	Основы управленческой деятельности Основы информационной безопасности Информационные технологии
ОПК-2	Основы управленческой деятельности Защита конфиденциального делопроизводства
ОПК-5	Теория информации
ОПК-6	Учебная ознакомительная практика Теория информации Основы управленческой деятельности
ОПК-8	Учебная ознакомительная практика Языки программирования Основы информационной безопасности
ОПК-10	Защита конфиденциального делопроизводства
ОПК-11	Дискретная математика
ОПК-12	Экономика
ОПК-4.3	Аппаратные средства вычислительной техники
ОПК-4.4	Аппаратные средства вычислительной техники

Таблица 3 – Требования к постреквизитам практики

Компетенция	Дисциплина/Практика

ОПК-2	Основы управления информационной безопасностью Организационное и правовое обеспечение информационной безопасности
ОПК-5	Организационное и правовое обеспечение информационной безопасности
ОПК-8	Программно-аппаратные средства защиты информации
ОПК-9	Защита информации от утечки по технических каналам Техническая защита информации Методы и средства криптографической защиты информации
ОПК-11	Защита информации от утечки по технических каналам
ОПК-4.1	Автоматизированные системы обработки информации
ОПК-4.3	Методы и средства криптографической защиты информации Аппаратные средства вычислительной техники
ОПК-4.4	Аппаратные средства вычислительной техники Автоматизированные системы обработки информации

5. ОБЪЕМ, ПРОДОЛЖИТЕЛЬНОСТЬ И СОДЕРЖАНИЕ ПРАКТИКИ

5.1 Время проведения практики согласно - календарного учебного графика.

5.2 Продолжительность практики составляет 2 недель.

5.3 Общая трудоёмкость учебной/производственной практики составляет 3 зачетных единиц.

Распределение по разделам/этапам практики, видам работ, форм текущего контроля с указанием номера осваиваемой компетенции в соответствии с ОПОП приведено в таблице 4.

Таблица 4. Распределение по разделам/этапам практики, видам работ, форм текущего контроля

Разделы (этапы) практики	Трудоёмкость					Результаты	
	Зач.ед.	Часов			Кол-во дней	форма текущего контроля	Коды формируемых компетенций, код индикатора достижения компетенции
		всего	контактная работа	Выполнение инд. задания			
Общая трудоемкость по учебному плану	3	108	72	36			
Раздел 1. Подготовительный							

1. Запись в дневнике практики		36	24	12			ОПК-4.1.1, ОПК-4.1.3, ОПК-4.4.2, ОПК-1.1, ОПК-1.3, ОПК-6.3, ОПК-8.1, ОПК-8.2, ОПК-8.3, ОПК-2.2, ОПК-2.3, ОПК-10.1, ОПК-10.2, ОПК-10.3, ОПК-11.1, ОПК-11.2, ОПК-11.3, ОПК-12.1, ОПК-12.2, ОПК-12.3
2. Запись в дневнике практики		36	24	12			ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ОПК-4.3.1, ОПК-4.3.2, ОПК-4.3.3, ОПК-4.3.4, ОПК-4.4.1, ОПК-4.4.2, ОПК-4.4.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4, ОПК-6.1, ОПК-6.2, ОПК-6.3, ОПК-8.1, ОПК-8.2, ОПК-8.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-9.1, ОПК-9.2, ОПК-9.3, ОПК-10.1, ОПК-10.2, ОПК-10.3, ОПК-11.1, ОПК-11.2, ОПК-11.3, ОПК-12.1, ОПК-12.2, ОПК-12.3
Раздел 3. Отчетный							

3. Выполнение определённых видов деятельности в рамках практики, осуществляемой на предприятии		36	24	12			ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ОПК-4.3.1, ОПК-4.3.2, ОПК-4.3.3, ОПК-4.3.4, ОПК-4.4.1, ОПК-4.4.2, ОПК-4.4.3, ОПК-1.1, ОПК -1.2, ОПК-1.3, ОПК-5.1, ОПК -5.2, ОПК-5.3, ОПК-5.4, ОПК -6.1, ОПК-6.2, ОПК-6.3, ОПК -8.1, ОПК-8.2, ОПК-8.3, ОПК -2.1, ОПК-2.2, ОПК-2.3, ОПК -2.4, ОПК-9.1, ОПК-9.2, ОПК -9.3, ОПК-10.1, ОПК-10.2, ОПК-10.3, ОПК-11.1, ОПК-11.2, ОПК-11.3, ОПК-12.1, ОПК-12.2, ОПК-12.3
Вид контроля	Зачет с оценкой						

5.3 Выполнение индивидуального задания студентов на практике.

1. Задачи производственной практики
2. Политики информационной безопасности в организации
3. Аппаратная и программная защита в организации
4. Информационная безопасность сетевых технологий организации
5. Система охранно-пожарной сигнализации и система видеонаблюдения
6. Системы контроля доступа (СКУД)
7. Предложения по совершенствованию практики
8. Вывод

1. Разработка системы защиты персональных данных в АС (общая характеристика, как объекта ИБ, состав и структура АС, как объекта ИБ, требования к системе защиты персональных данных в АС). 2. Разработка подсистемы программно- аппаратной защиты информации для КСЗИ ЛВС малого коммерческого предприятия»

3. Проект по совершенствованию системы защищенного электронного документооборота при использовании «облачных» технологий.

4. Совершенствование методики управления инцидентами в проектных решениях.

5. Совершенствование методики управления информационными рисками при

реализации проектных решений.

6. «Разработка проекта системы ЗИ для распределенной вычислительной сети в учреждении здравоохранения»

7. Разработка усовершенствованной подсистемы СКУД типового предприятия (описание объекта, проектирование системы контроля и управления доступом, структурно –функциональная схема усовершенствованной СКУД, технология установки).

8. Проектирование системы ИТЗИ кабинета руководителя среднего госпредприятия.

9. Анализ существующей системы ИТЗИ кабинета руководителя госпредприятия

10. Организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации

11. Оценка эффективности предлагаемой системы инженерно-технической защиты кабинета руководителя госпредприятия.

12. Разработка системы информационной безопасности.

13. Разработка автоматизированной системы аудита защиты персональных данных высшего учебного учреждения (на примере Университета).

14. Разработка облика целесообразной подсистемы аудита защиты персональных данных.

15. Разработать перечень мероприятий по устранению выявленных недостатков подсистемы компьютерной безопасности.

16. Разработка автоматизированной подсистемы управления защитой персональных данных в.

17. Разработать перечень мероприятий по устранению и ограничению недостатков системы защиты информации предприятия, выработать предложения о возможности внедрения дополнительных мер.

18. Разработка подсистемы компьютерной безопасности для малого коммерческого предприятия.

19. Разработка проекта подсистемы защиты персональных данных в информационной системе. 20. Разработка основ методологии выявления и оценки деструктивных воздействий в подсистеме энергоинформационной безопасности типового предприятия.

21. Организация защиты персональных данных на объектах информатизации.

22. Организация защиты конфиденциальной информации в организации и обеспечение безопасности информации в современных условиях.

23. Разработка политики информационной безопасности в условиях автоматизации деятельности 24. Разработка коммерческого продукта – системы защиты авторского права для учреждений.

25. Проект по совершенствованию системы программно-аппаратной защиты информации автоматизированного рабочего места сотрудника.

26. Проектирование системы защиты конфиденциальной при использовании «облачных» технологий.

27. Проект по совершенствованию системы физической защиты информационных объектов торгового предприятия.

28. Разработка коммерческого продукта анализа открытых персональных данных в сети Интернет. 29. Разработка методики организации тестового режима работы видеосистем стандарта DVI при проведении контроля защищённости информации от утечки по каналам ПЭМИН.

30. Разработка проекта подсистемы сетевого аудита информационной безопасности основных компонентов ЛВС крупного промышленного предприятия.

31. Совершенствование подсистемы инженерно-технической защиты информации технических средств связи выделенного помещения типового предприятия.

32. Создание подсистемы физической защиты информации для типового заведения.

6. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

6.1 По окончании практики обучающийся должен предоставить на кафедру следующие документы не позднее 7 календарных дней с даты начала занятий или окончания практики:

- заполненный дневник с отзывом (оценкой работы практиканта администрацией и старшим специалистом предприятия). Дневник должен быть заверен подписью ответственного лица и круглой печатью организации;
- отчет по практике. Отчет по практики подписывается обучающимся, проверяется и визируется руководителем практики. Защита отчетов производится в соответствии с установленным графиком защиты отчетов, но не позднее трех месяцев с начала учебного процесса. Нарушение сроков прохождения практики и сроков защиты считается невыполнением учебного плана. По результатам защиты отчетов, а также отзыва с места прохождения практики обучающимся выставляется оценка по практике;
- индивидуальное задание.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

7.1 Форма аттестации практики Зачет с оценкой.

7.2 Время проведения аттестации с 29.06.2022 г. по 12.07.2022 г.

7.3 Зачет получает обучающийся, прошедший практику, представивший Отчет и успешно защитивший отчет по практике.

7.4 Описание системы оценок.

7.4.1 По результатам прохождения практики начисляется максимум 100 балов.

7.4.2 Критерии балльно-рейтинговой оценки результатов прохождения обучающимися практики формируются на кафедре, за которой закреплена дисциплина. Перечень критериев зависит от специфики практики.

Основные критерии:

- полнота представленного материала, выполнение индивидуального задания, соответствующие программе практики – до 50 баллов;
- своевременное представление отчета, качество оформления – до 20 баллов;
- защита отчета, качество ответов на вопросы – до 30 баллов.

Форма фиксации с возможным вариантом критериев представлена в таблице 5.

Таблица 5. Структура формирования балльно-рейтинговой оценки результатов прохождения обучающимися практики

№	Критерии оценок	Баллы
1	полнота представленного материала, выполнение индивидуального задания	25
2	соответствие представленных результатов программе практики	25
3	своевременное представление отчета	10
4	качество оформления отчета	10
5	доклад по отчету	20
6	качество ответов на дополнительные вопросы	10
	ИТОГО	100

7.4.3 Структура формирования балльно-рейтинговой оценки прохождения обучающимися практики определяется ведущим преподавателем, рассматривается и одобряется на заседании кафедры, утверждается в установленном порядке в составе программы практики.

7.4.4 Система оценок представлена в таблице 6.

Таблица 6. Система оценок

Диапазон оценки в баллах	европейская шкала (ECTS)	традиционная шкала	**Зачет**
[95;100]	A - (5+)	отлично – (5)	зачтено
[85; 95)	B - (5)		
[70; 85)	C– (4)	хорошо – (4)	
[60; 70)	D– (3+)	удовлетворительно – (3)	
[50; 60)	E– (3)		незачтено
[33,3; 50)	FX– (2+)	неудовлетворительно – (2)	
[0; 33,3)	F– (2)		

7.4.5 Прохождение всех этапов практики (выполнение всех видов работ) является обязательным. Набрав высокий балл за один из этапов практики, обучающийся не освобождается от прохождения других этапов.

7.4.6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике.

8. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

8.1.1 Основная учебная литература, необходимая для освоения дисциплины

Бердникова, Л. Н. Технологическая практика : методические указания / Л. Н. Бердникова. — Красноярск : КрасГАУ, 2020. — 20 с. — Текст : электронный // Лань : электронно-библиотечная система.

8.1.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Логистика и управление цепями поставок : методические указания / составитель Е. О. Чебакова. — Омск : СибАДИ, 2022. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система.
2. Кадушкин, Ю. В. Технологическая практика : методические указания / Ю. В. Кадушкин. — Санкт-Петербург : СПбГАУ, 2019. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система.
3. Юрков, Н. К. Технология производства электронных средств : учебник / Н. К. Юрков. — 2-е изд., испр., доп. — Санкт-Петербург : Лань, 2021. — 480 с. — ISBN 978-5-8114-1552-6. — Текст : электронный // Лань : электронно-библиотечная система.

8.1.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисциплины

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

9.1 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

9.2 Современные профессиональные базы данных и информационно-справочные системы

1. Консуультант+.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

ПК, стандартные офисные программные средства

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Заведующий кафедрой,к.т.н. _____ Урбан Владимир Александрович

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 7 от 22.02.2021 г.

Директор Института управления рисками и комплексной безопасности

_____ Яковлева Евгения Васильевна