

<p>Цель и задачи изучения дисциплины:</p>	<p>Практика обеспечивает соответствие уровня теоретической подготовки практической направленности в системе обучения и будущей деятельности выпускника.</p> <p>Цель практики:</p> <ul style="list-style-type: none"> – закрепление, расширение, углубление и систематизация знаний, полученных при изучении обязательных дисциплин базовой части учебного плана; – освоение современных технологий и технических средств, применяемых в области информационной безопасности; – совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики; – обеспечение возможности применения студентами теоретических знаний для решения практических задач; – развитие организаторских способностей и развитие исполнительских и лидерских навыков обучающихся; – формирование и развитие практических навыков в профессиональной сфере использования технологий и технических средств, применяемых в области информационной безопасности; – развитие у обучающихся компетенций, а также формирования опыта самостоятельной исследовательской и аналитической деятельности в изучении практического материала; – формирование общего представления студентов о будущей профессиональной деятельности и развитие интереса к профессии.
<p>Место дисциплины в структуре ОПОП</p>	<p>Производственная практика: технологическая практика относится к обязательной части Блока 2 образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность</p>
<p>Краткая характеристика учебной дисциплины (основные блоки, темы)</p>	<p>Содержание практики:</p> <p>Подготовительный этап Установочная конференция:</p> <p>цели и задачи учебной практики; инструктаж по технике безопасности; получение задания на практику (в том числе – индивидуальные варианты); требования к оформлению документов (отчет, дневник и пр.)</p> <p>Содержательный этап Выполнение практических работ Выполнение индивидуального задания</p> <p>Отчетный этап Подготовка и оформление отчета по практике</p>

<p>Компетенции, формируемые в результате освоения учебной дисциплины:</p>	<p>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;</p> <p>ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;</p> <p>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;</p> <p>ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;</p> <p>ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;</p> <p>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;</p> <p>ПК-1: Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем;</p> <p>ПК-2: Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности;</p> <p>ПК-3: Способен обеспечивать безопасную обработку данных в автоматизированных системах;</p> <p>ПК-6: Способен документально оформлять работы по обеспечению информационной безопасности.</p>
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины:</p>	<p>ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации</p> <p>ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа</p> <p>ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации</p> <p>ОПК-6.4: Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации</p> <p>ОПК-9.1: Использует средства криптографической</p>

	<p>защиты информации в автоматизированных системах</p> <p>ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов</p> <p>ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации</p> <p>ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации</p> <p>ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации</p> <p>ОПК-10.1: Реализует требования политик безопасности на объектах информатизации</p> <p>ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности</p> <p>ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях</p> <p>ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите</p> <p>ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации</p> <p>ОПК-12.3: Оценивает информационные риски в автоматизированных системах</p> <p>ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений</p> <p>ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем</p> <p>ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе</p> <p>ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации</p> <p>ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации</p> <p>ОПК-4.3.1: Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы</p> <p>ОПК-4.3.2: Применяет программные средства обеспечения безопасности данных</p> <p>ОПК-4.3.3: Управляет полномочиями пользователей автоматизированной системы</p> <p>ПК-1.1: Производит внедрение в состав</p>
--	---

	<p>автоматизированных систем средств обеспечения информационной безопасности</p> <p>ПК-1.2: Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности</p> <p>ПК-1.3: Выполняет регламентные работы по эксплуатации средств защиты информации</p> <p>ПК-1.4: Устраняет неисправности при эксплуатации средств защиты информации</p> <p>ПК-2.1: Формулирует критерии безопасности обработки информации в автоматизированных системах</p> <p>ПК-2.2: Выполняет мероприятия для реализации политики информационной безопасности</p> <p>ПК-2.3: Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД</p> <p>ПК-2.4: Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД</p> <p>ПК-2.5: Устанавливает программное обеспечение в соответствии с требованиями по защите информации</p> <p>ПК-3.1: Фиксирует возникновение инцидентов информационной безопасности</p> <p>ПК-3.2: Использует методы и средства резервного копирования информации</p> <p>ПК-3.3: Устраняет уязвимости в автоматизированной системе</p> <p>ПК-3.4: Соотносит изменения в конфигурации автоматизированной системы с её защищенностью</p> <p>ПК-6.1: Анализирует полноту и нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности</p> <p>ПК-6.2: Формирует отчетные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации</p> <p>ПК-6.3: Формулирует в соответствии с требованиями руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации</p> <p>ПК-6.4: Готовит документы для проведения работ по аттестации объектов информатизации и автоматизированных систем</p>
<p>Формы проведения занятий, образовательные технологии:</p>	<p>Способы проведения практики – стационарная, выездная. Формы проведения практики – дискретно: путем чередования в календарном учебном графике периодов учебного времени для проведения практик с периодами учебного времени для проведения теоретических занятий.</p> <p>Технологии: метод «коллективной мыслительной деятельности», методы анализа проблемных ситуаций, логико-методологическое проектирование, решение</p>

	задач.
Используемые инструментальные и программные средства:	Средства проекции (презентации), программированного контроля (тестирования), средства защиты информации
Формы промежуточного контроля:	Текущие оценки знаний, тестирование, доклады, самостоятельные работы
Общая трудоемкость изучения дисциплины:	108 ч./ 3 з.е.
Форма итогового контроля знаний:	Зачет с оценкой