

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА**

**Институт физико-математических наук и информационных технологий**

«Согласовано»

Ведущий менеджер ООП ИФМНиИТ  
В.И.Бурмистров

«10» марта 2020 г.

«Утверждено»

Директор ИФМНиИТ  
А.В.Юров

«10» марта 2020 г.



**ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРЕДИПЛОМНОЙ ПРАКТИКИ**

для студентов 4 курса  
очной формы обучения

направления подготовки 10.03.01.

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

профиль подготовки **«ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ  
ИНФОРМАЦИИ»**

уровень высшего образования – бакалавриат

Калининград, 2020 г.

## Лист согласования

**Составители:** доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

Программа обсуждена и утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий.

Протокол № \_\_\_/\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Председатель учебно-методического совета \_\_\_\_\_ первый  
заместитель директора института, к.ф.-м.н., доцент, Шпилевой А. А.

Программа пересмотрена на заседании учебно-методического совета института физико-математических наук и информационных технологий. Внесены следующие изменения (или изменений не внесено) \_\_\_\_\_

Протокол № \_\_\_\_\_ от « \_\_\_ » \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП \_\_\_\_\_ Бурмистров В. И.

СОДЕРЖАНИЕ  
ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРЕДДИПЛОМНОЙ  
ПРАКТИКИ

1. Указание вида практики, способа и формы ее проведения.....	4
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.....	4
3. Указание места практики в структуре образовательной программы.....	12
4. Указание объема практики в зачетных единицах и ее продолжительности в неделях и академических часах.....	17
5. Содержание практики.....	17
6. Указание форм отчетности по практике.....	17
7. Фонд оценочных средств проведения промежуточной аттестации обучающихся по практике.....	18
7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках производственной преддипломной практики.....	18
7.2 Показатели и критерии оценивания компетенций на различных этапах их формирования.....	25
7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в рамках производственной преддипломной практики.....	30
7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.....	33
8. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики.....	36
9. Перечень информационных технологий, используемых при проведении практики.....	38
10. Описание материально-технической базы, необходимой для проведения практики.....	39
Приложение 1.....	41

## **1. УКАЗАНИЕ ВИДА ПРАКТИКИ, СПОСОБА И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ**

**Вид практики:** производственная практика.

**Способ проведения** производственной практики: стационарная.

Стационарная практика проводится в образовательной организации, в которой обучающиеся осваивают образовательную программу, или в иных организациях, с которыми действуют соответствующие договорные отношения.

**Формы проведения** производственной практики: невыездная, непрерывная. Организация проведения производственной преддипломной практики осуществляется путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения практики.

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

**Цели производственной преддипломной практики:**

-закрепление знаний и умений, полученных в процессе теоретического обучения, овладение методикой обеспечения информационной безопасности предприятия (организации), проектирования, внедрения и эксплуатации отдельных задач и подсистем комплексной системы защиты информации предприятия (организации).

-приобретение практических навыков работы в качестве специалиста ИБ предприятия (организации); приобретение навыков обслуживания средств ЗИ в ЭВМ, сетях ЭВМ и автоматизированных информационных системах; приобретение практического опыта разработки компонентов КСЗИ предприятия (организации);

- приобретение навыка системного подхода при проектировании КСЗИ и отдельных ее подсистем;

- приобретение навыков исследовательской и аналитической работы в области информационной безопасности.
- приобретение практических навыков и опыта самостоятельной профессиональной деятельности.
- сбор необходимых материалов для написания выпускной квалификационной работы
- приобщение студента к социальной среде предприятия с целью приобретения социально-личностных компетенций, необходимых для работы в профессиональной сфере

К основным задачам производственной преддипломной практики относятся:

- приобретение практических навыков работы в качестве специалиста информационной безопасности предприятия (организации);
- изучение методов обеспечения безопасности информации, применяемых на предприятии (в организации);
- освоение на практике методов предпроектного обследования объектов информатизации, проведения системного анализа результатов обследования при построении модели комплексной системы защиты информации;
- приобретение практического опыта разработки компонентов комплексной системы защиты информации предприятия (организации);
- изучение технологии регистрации, сбора, передачи и обработки информации о несанкционированных действиях, ознакомление с характеристиками периферийной, терминальной и вычислительной техники и особенностями их эксплуатации в условиях функционирования аппаратно-программных компонентов подсистем комплексной системы защиты информации;
- изучение документации комплексной системы защиты информации предприятия (организации), получение знаний по оформлению технических и рабочих проектов системы защиты информации и порядку внедрения утвержденных решений;

привитие навыка системного подхода при проектировании комплексной системы защиты информации и отдельных ее подсистем;

-написание выпускной квалификационной работы.

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Результаты освоения ООП	Перечень планируемых результатов обучения по дисциплине
ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	<p><b>Знать:</b> способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации;</p> <p><b>Уметь:</b> классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения</p> <p><b>Владеть:</b> навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>

ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	<p><b>Знать:</b> основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий;</p> <p><b>Уметь:</b> определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий</p> <p><b>Владеть:</b> методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей</p>
ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	<p><b>Знать:</b> задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p><b>Уметь:</b> применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять</p>

		<p>критерии эффективности работы средств защиты информации;</p> <p>обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p><b>Владеть:</b></p> <p>средствами защиты информации в процессе хранения и передачи данных и методами их тестирования;</p> <p>методикой определения эффективности предложенных решений с учетом снижения рисков</p>
ПК-4	<p>Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p><b>Знать:</b></p> <p>этапы и модели жизненного цикла информационных систем;</p> <p>корпоративные стандарты и методики;</p> <p>принципы хранения, защиты, передачи и получения информации в корпоративных сетях</p> <p><b>Уметь:</b></p> <p>разрабатывать структуру распределенных систем;</p> <p>создавать клиент-серверные приложения для распределенных систем;</p> <p>проектировать хранилища данных;</p> <p>выполнять анализ корпоративных данных</p> <p><b>Владеть:</b></p> <p>навыками защиты информации в корпоративных сетях связи</p>
ПК-5	<p>Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации</p>	<p><b>Знать:</b></p> <p>правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;</p> <p>правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;</p> <p>основные отечественные и зарубежные стандарты в области компьютерной безопасности</p> <p><b>Уметь:</b></p> <p>применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности;</p> <p>разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности;</p>



		<p>разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем</p> <p><b>Владеть:</b></p> <p>навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках</p>
ПК-6	<p>Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p>	<p><b>Знать:</b></p> <p>методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности; этапы и процедуры аудита информационной безопасности автоматизированных систем управления</p> <p><b>Уметь:</b></p> <p>разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления</p> <p><b>Владеть:</b></p> <p>способами контроля эффективности реализации политики информационной безопасности организации; анализом недостатков в функционировании системы защиты информации автоматизированной системы; способами оценки защищённости автоматизированной системы; методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления</p>

		нормативным требованиям по защите информации
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	<p><b>Знать:</b>  архитектуру основных типов современных компьютерных систем;  структуру и принципы работы современных и перспективных микропроцессоров;  принципы работы элементов и функциональных узлов электронной аппаратуры;  принципы построения и работы ПЭВМ</p> <p><b>Уметь:</b>  определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств;  работать с современной элементной базой электронной аппаратуры.  определять направления использования ЭВМ определенного класса для решения служебных задач</p> <p><b>Владеть:</b>  навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности;  навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования;  навыками формирования структуры СВТ и выбора режимов их функционирования</p>
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	<p><b>Знать:</b>  терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности в компьютерной сфере</p> <p><b>Уметь:</b>  пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;  отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации</p> <p><b>Владеть:</b>  навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы;  с технической документацией на компоненты</p>

		компьютерных систем на русском и иностранном языках
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	<p><b>Знать:</b> направления создания правовой базы в области информационной безопасности; области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну</p> <p><b>Уметь:</b> разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов</p> <p><b>Владеть:</b> навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации</p>
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	<p><b>Знать:</b> основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности</p> <p><b>Уметь:</b> определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять</p>

		<p>системы компьютерной математики для решения типовых задач</p> <p><b>Владеть:</b></p> <p>способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации;</p> <p>навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации</p>
ПК-11	<p>Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов</p>	<p><b>Знать:</b></p> <p>физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации;</p> <p>основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности;</p> <p><b>Уметь:</b></p> <p>использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;</p> <p>решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;</p> <p>проводить классификацию экспериментов; выполнять оптимальное планирование</p>

		<p>экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач</p> <p><b>Владеть:</b>  навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну</p>
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	<p><b>Знать:</b>  основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной</p>

		<p>неопределенности имеющейся информации</p> <p><b>Уметь:</b> разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задач защиты информации</p> <p><b>Владеть:</b> методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации</p>
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	<p><b>Знать:</b> типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации;</p> <p><b>Уметь:</b> определять состав компьютера: тип процессора и его параметры, тип модулей</p>

		<p>памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры.</p> <p>определять направления использования ЭВМ определенного класса для решения служебных задач</p> <p><b>Владеть:</b></p> <p>навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности;</p> <p>навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования;</p> <p>навыками формирования структуры СВТ и выбора режимов их функционирования</p>
ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	<p><b>Знать:</b></p> <p>назначение, виды и принципы построения организации и управления службы защиты информации</p> <p><b>Уметь:</b></p> <p>применять современные компьютерные технологии для решения профессиональных задач;</p> <p>ориентироваться в сети научных и образовательных порталов сети Интернет;</p> <p>обрабатывать результаты полученных измерений с помощью математических программных продуктов</p> <p><b>Владеть:</b></p> <p>навыками работы с пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информацией</p>
ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	<p><b>Знать:</b></p> <p>основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности;</p> <p>технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи</p>

		<p>информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии</p> <p><b>Уметь:</b>  осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;  организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;  анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации</p> <p><b>Владеть:</b>  навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации</p>
ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построения карьеры и/или педагогики	<p><b>Знать:</b>  теоретические основы построения клиент-серверных веб-приложений, общие методы программирования  механизмы реализации сетевых угроз по протоколам передачи данных HTTP, FTP, а также известные уязвимости веб-серверов</p> <p><b>Уметь:</b>  использовать полученные теоретические знания для решения конкретных прикладных задач, программировать клиент-серверные приложения с применением СУБД для обработки данных, находить и исправлять ошибки в программном коде  конфигурировать клиент-серверное программное обеспечение с учетом требуемых параметров сетевой безопасности, анализировать возможные каналы утечки информации</p>



		<b>Владеть:</b> практическими навыками конфигурирования и администрирования веб-серверов, а также навыками настройки систем управления контентом практическими навыками, по оценке защищенности веб-приложений
--	--	--

### 3. УКАЗАНИЕ МЕСТА ПРОИЗВОДСТВЕННОЙ ПРЕДДИПЛОМНОЙ ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Производственная преддипломная практика представляет собой дисциплину вариативной части (Б2.В.04(Пд)) блока Б2 «Практика» подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность» по профилю подготовки «Организация и технология защиты информации».

Логическая и содержательная связь дисциплин, участвующих в формировании представленных в п.1 компетенций, содержится в ниже представленной таблице:

Код компетенции	Предшествующие дисциплины	Данная дисциплина	Последующие дисциплины
ПК-1	Теоретические основы компьютерной безопасности Криптографические методы защиты информации Техническая защита информации Программно-аппаратные средства защиты информации Распространение электромагнитных волн и антенно-фидерные устройства Основы электромагнитной совместимости Основы построения многоканальных инфокоммуникационных систем и сетей Сети и системы передачи информации Аппаратные средства	Производственная преддипломная практика	Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы

	<p>вычислительной техники          Производственная эксплуатационная практика          Криптографические протоколы          Защита в операционных системах          Криптографические протоколы для защиты банковской информации</p>		
ПК-2	<p>Языки программирования          Операционные системы          Базы данных          Теоретические основы компьютерной безопасности          Цифровая обработка сигналов          Криптографические методы защиты информации          Программно-аппаратные средства защиты информации          Учебная практика по получению первичных профессиональных умений и навыков          Производственная эксплуатационная практика          Криптографические протоколы          Защита в операционных системах          Защита программ и данных          Основы построения защищенных баз данных          Криптографические протоколы для защиты банковской информации          Надежность, эргономика и качество информационных систем</p>		<p>Подготовка к процедуре защиты выпускной квалификационной работы          Процедура защиты выпускной квалификационной работы</p>
ПК-3	<p>Операционные системы          Базы данных</p>		<p>Подготовка к процедуре защиты</p>

	<p>Теоретические основы компьютерной безопасности          Программно-аппаратные средства защиты информации          Производственная эксплуатационная практика          Информационная безопасность корпоративных сетей          Защита персональных данных в организации          Аудит информационной безопасности автоматизированных систем          Защита информации в кредитно-финансовых организациях          Управление информационной безопасностью          Стандарты информационной безопасности          Организация и управление службой защиты информации          Информационная безопасность автоматизированных систем</p>		<p>выпускной квалификационной работы          Процедура защиты выпускной квалификационной работы</p>
ПК-4	<p>Основы управления информационной безопасности          Информационная безопасность корпоративных сетей          Документоведение          Учебная практика по получению первичных профессиональных умений и навыков          Производственная эксплуатационная практика          Защита и обработка конфиденциальных документов</p>		<p>Подготовка к процедуре защиты выпускной квалификационной работы          Процедура защиты выпускной квалификационной работы</p>

	<p>Защита персональных данных в организации  Аудит информационной безопасности автоматизированных систем  Защита информации в кредитно-финансовых организациях  Управление информационной безопасностью  Стандарты информационной безопасности  Организация и управление службой защиты информации  Информационная безопасность автоматизированных систем  Производственная эксплуатационная практика</p>		
ПК-5	<p>Основы управления информационной безопасности  Организационное и правовое обеспечение информационной безопасности  Информационная безопасность корпоративных сетей  Документоведение  Производственная эксплуатационная практика  Защита и обработка конфиденциальных документов  Управление информационной безопасностью  Стандарты информационной безопасности  Организация и управление службой защиты информации</p>		<p>Подготовка к процедуре защиты выпускной квалификационной работы  Процедура защиты выпускной квалификационной работы</p>

	Информационная безопасность автоматизированных систем		
ПК-6	<p>Основы управления информационной безопасности</p> <p>Организационное и правовое обеспечение информационной безопасности</p> <p>Техническая защита информации</p> <p>Программно-аппаратные средства защиты информации</p> <p>Аппаратные средства вычислительной техники</p> <p>Производственная эксплуатационная практика</p> <p>Управление информационной безопасностью</p> <p>Стандарты информационной безопасности</p> <p>Организация и управление службой защиты информации</p> <p>Информационная безопасность автоматизированных систем</p>		<p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p>
ПК-7	<p>Организационное и правовое обеспечение информационной безопасности</p> <p>Производственная эксплуатационная практика</p> <p>Информационная безопасность корпоративных сетей</p> <p>Защита персональных данных в организации</p> <p>Аудит информационной безопасности автоматизированных систем</p>		<p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p>

	<p>Криптографические протоколы  Защита информации в кредитно-финансовых организациях  Защита программ и данных  Основы построения защищенных баз данных  Криптографические протоколы для защиты банковской информации  Надежность, эргономика и качество информационных систем  Производственная проектно-технологическая практика</p>		
ПК-8	<p>Основы управления информационной безопасности  Организационное и правовое обеспечение информационной безопасности  Метрология, стандартизация и сертификация  Учебная практика по получению первичных профессиональных умений и навыков  Производственная эксплуатационная практика  Производственная проектно-технологическая практика</p>		<p>Подготовка к процедуре защиты выпускной квалификационной работы  Процедура защиты выпускной квалификационной работы  Астрономия и астрофизика  Космология</p>
ПК-9	<p>Основы информационной безопасности  Квантовые методы защиты и обработки информации  Учебная практика по получению первичных профессиональных умений и навыков  Производственная</p>		<p>Подготовка к процедуре защиты выпускной квалификационной работы  Процедура защиты выпускной квалификационной работы</p>

	эксплуатационная практика		
ПК-10	Организационное и правовое обеспечение информационной безопасности Производственная эксплуатационная практика		Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-11	Техническая защита информации Аппаратные средства вычислительной техники Производственная эксплуатационная практика		Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-12	Техническая защита информации Аппаратные средства вычислительной техники Производственная эксплуатационная практика		Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-13	Техническая защита информации Аппаратные средства вычислительной техники Производственная эксплуатационная практика		Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-14	Основы управления информационной безопасности Элективные курсы по физической культуре и спорту Производственная эксплуатационная практика		Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-15	Основы управления информационной безопасности Производственная эксплуатационная практика		Подготовка к процедуре защиты выпускной квалификационной работы

	практика		Процедура защиты выпускной квалификационной работы
ПКУ-1	Модуль личностно-ориентированного совершенствования Модуль предпринимательский Модуль педагогический Модуль информационно-технологический Модуль коммуникационный		Подготовка к процедуре защиты выпускной квалификационной работы

#### **4. УКАЗАНИЕ ОБЪЕМА ПРАКТИКИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТИ В НЕДЕЛЯХ И АКАДЕМИЧЕСКИХ ЧАСАХ.**

Производственная преддипломная практика проводится в 8-м учебном семестре в течение 6 недель. Трудоемкость учебной практики - 9 зачетных единиц (ЗЕ) и 324 академических часа.

#### **5. СОДЕРЖАНИЕ ПРАКТИКИ**

<b>№ п/п</b>	<b>Этапы практики</b>	<b>Виды работы</b>	<b>Трудоёмкость, час.</b>
1	Подготовительный (ознакомительный) этап	Проведение организационного собрания. Получение задания на практику. Ознакомление с заданием, планирование работы. Проведение инструктажа по ОТ и ТБ на рабочем месте.	2
2	Подготовка теоретических материалов.	Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических указаний и т.д.	108
3	Практические работы по теме задания на практику	Проведение практических работ (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования и др.	198
4	Отчёт по практике	Составление отчёта по практике	16



<b>Итого 9 З.Е.</b>		<b>324</b>
<b>* ЗЕ -зачетная единица</b>		

## **6. УКАЗАНИЕ ФОРМ ОТЧЕТНОСТИ ПО ПРАКТИКЕ**

Студент выполняет программу производственной преддипломной практики в соответствии с планом-графиком практики и индивидуальным заданием на практику, утверждаемым учебно-методическим советом института, ведет дневник практики, который защищает после окончания практики. В зависимости от специализации подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Для текущего контроля посещаемости производственной преддипломной практики используется стандартный журнал посещения занятий, который будет вести руководитель практики.

Отчет о результатах прохождения производственной преддипломной практики заслушивается на заседании учебно-методического совета института.

Дневник производственной эксплуатационной практики представлен в Приложении 1.

## **7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ**

### **7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках производственной эксплуатационной практики**

Контролируемые модули, разделы (темы) практики	Индекс контролируемой компетенции (или её части)	Содержание компетенции	Оценочные средства по этапам формирования компетенций	
			Текущий контроль по практике	промежуточный контроль по практике
Подготовительный	ПК-1	Способностью выполнять	Устный	

<p>(ознакомительный) этап. Проведение организационного собрания. Получение задания на практику. Ознакомление с заданием, планирование работы. Проведение инструктажа по ОТ и ТБ на рабочем месте.</p>		работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	опрос, собеседование, консультации	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос, собеседование, консультации	
	ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	Устный опрос, собеседование, консультации	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос, собеседование, консультации	
	ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Устный опрос, собеседование, консультации	
	ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Устный опрос, собеседование, консультации	
	ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос, собеседование, консультации	
	ПК-8	Способностью оформлять рабочую техническую документацию с учетом	Устный опрос,	

	действующих нормативных и методических документов	собеседование, консультации	
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос, собеседование, консультации	
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Устный опрос, собеседование, консультации	
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Устный опрос, собеседование, консультации	
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Устный опрос, собеседование, консультации	
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Устный опрос, собеседование, консультации	
ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Устный опрос, собеседование, консультации	
ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной	Устный опрос, собеседование, консультации	

		службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		
	ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построения карьеры и/или педагогики	Устный опрос, собеседование, консультация	
Подготовка теоретических материалов. Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических указаний и т.д. Практические работы по теме задания на практику	ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Устный опрос, собеседование, консультация	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос, собеседование, консультация	
	ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	Устный опрос, собеседование, консультация	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос, собеседование, консультация	
	ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Устный опрос, собеседование, консультация	
	ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических	Устный опрос, собеседование, консультация	

		средств защиты информации		
ПК-7		Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос, собеседование, консультации	
ПК-8		Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос, собеседование, консультации	
ПК-9		Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос, собеседование, консультации	
ПК-10		Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Устный опрос, собеседование, консультации	
ПК-11		Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Устный опрос, собеседование, консультации	
ПК-12		Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Устный опрос, собеседование, консультации	
ПК-13		Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Устный опрос, собеседование, консультации	
ПК-14		Способностью организовывать работу малого коллектива	Устный опрос,	

		исполнителей в профессиональной деятельности	собеседование, консультации	
	ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Устный опрос, собеседование, консультации	
	ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики	Устный опрос, собеседование, консультации	
Практические работы по теме задания на практику. Проведение практических работ (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования и др.	ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Устный опрос, собеседование, консультации	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос, собеседование, консультации	
	ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	Устный опрос, собеседование, консультации	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос, собеседование, консультации	
	ПК-5	Способностью принимать	Устный	

		участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	опрос, собеседование, консультации	
	ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Устный опрос, собеседование, консультации	
	ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос, собеседование, консультации	
	ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос, собеседование, консультации	
	ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос, собеседование, консультации	
	ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Устный опрос, собеседование, консультации	
	ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Устный опрос, собеседование, консультации	
	ПК-12	Способностью принимать участие в проведении экспериментальных	Устный опрос,	

		исследований системы защиты информации	собеседование, консультации	
	ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Устный опрос, собеседование, консультации	
	ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Устный опрос, собеседование, консультации	
	ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Устный опрос, собеседование, консультации	
	ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики	Устный опрос, собеседование, консультации	
Отчёт по практике. Составление отчёта по практике.	ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Устный опрос, собеседование, консультации	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос, собеседование, консультации	



	ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	Устный опрос, собеседование, консультации	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос, собеседование, консультации	
	ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Устный опрос, собеседование, консультации	
	ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Устный опрос, собеседование, консультации	
	ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос, собеседование, консультации	
	ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос, собеседование, консультации	
	ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос, собеседование, консультации	
	ПК-10	Способностью проводить анализ информационной безопасности	Устный опрос,	

		объектов и систем на соответствие требованиям стандартов в области информационной безопасности	собеседование, консультация	
	ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Устный опрос, собеседование, консультация	
	ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Устный опрос, собеседование, консультация	
	ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Устный опрос, собеседование, консультация	
	ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Устный опрос, собеседование, консультация	
	ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Устный опрос, собеседование, консультация	
	ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики	Устный опрос, собеседование, консультация	
				зачет

**Этапы формирования компетенций в процессе освоения образовательной программы в рамках производственной преддипломной практики**

Индекс контролируемой компетенции	№ Учебной недели № Темы раздела дисциплины/модуля								
	33	33	34	35	35	36	37	38	38
	1	2	2	2	3	3	3	3	4
	Этапы формирования компетенции								
ПК-1	+	+	+	+	+	+	+	+	+
ПК-2	+	+	+	+	+	+	+	+	+
ПК-3	+	+	+	+	+	+	+	+	+
ПК-4	+	+	+	+	+	+	+	+	+
ПК-5	+	+	+	+	+	+	+	+	+
ПК-6	+	+	+	+	+	+	+	+	+
ПК-7	+	+	+	+	+	+	+	+	+
ПК-8	+	+	+	+	+	+	+	+	+
ПК-9	+	+	+	+	+	+	+	+	+
ПК-10	+	+	+	+	+	+	+	+	+
ПК-11	+	+	+	+	+	+	+	+	+
ПК-12	+	+	+	+	+	+	+	+	+
ПК-13	+	+	+	+	+	+	+	+	+
ПК-14	+	+	+	+	+	+	+	+	+
ПК-15	+	+	+	+	+	+	+	+	+
ПКУ-1	+	+	+	+	+	+	+	+	+

**7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования**  
**Критерии определения сформированности компетенций на различных этапах их формирования**

Показатели	ниже порогового	пороговый	достаточный	повышенный
<b>Критерии</b>	Компетенция не сформирована. Студент не способен определить основные понятия, воспроизвести основные факты, идеи теории информационной безопасности, не знает основные методы решения типовых задач. Не умеет работать со справочной литературой, не способен представить результаты своей работы. Не владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, не способен применять информационные технологии для решения типовых задач	Компетенция сформирована на «удовлетворительно». Студент дает определения основных понятий, воспроизводит основные факты, идеи, теории информационной безопасности, знает основные методы решения типовых задач. Умеет работать со справочной литературой, представлять результаты своей работы. Владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, способен применять информационные технологии для решения типовых задач	Компетенция сформирована на «хорошо». Студент понимает связи между различными понятиями теории, аргументирует выбор метода решения задачи и умеет их применять на практике. Применяет методы решения задач в незнакомых ситуациях, умеет корректно выражать и аргументированно обосновывать положения предметной области знания. Способен применять информационные технологии для решения прикладных задач, адаптировать типовые технологии к решению практико-ориентированных задач.	Компетенция сформирована «отлично». Студент устанавливает связи между основными концепциями в предметной области, теориями дисциплинами. Оценивает достоверность полученного решения задачи, методы решения задачи и выбирает оптимальный метод, разрабатывает модели реальных процессов и ситуаций. Способен передавать результат проведенных исследований в виде конкретных рекомендаций в терминах предметной области знания, интерпретировать знания предметной области.

Поскольку практически всякая учебная дисциплина призвана формировать сразу несколько компетенций, критерии оценки целесообразно формировать в два этапа.

1-й этап: определение критериев оценки отдельно по каждой формируемой компетенции. Сущность 1-го этапа состоит в определении шкал оценивания для оценивания отдельно взятой компетенции на основе продемонстрированного обучаемым уровня самостоятельности в применении полученных в ходе изучения учебной дисциплины, знаний, умений и навыков.

## Шкала оценивания компетенций

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины</p>	<p>Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне</p>	<p>Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке</p>	<p>Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи</p>

2-й этап: определение критериев для оценки уровня обученности по учебной дисциплине на основе комплексного подхода к уровню сформированности всех компетенций, обязательных к формированию в процессе изучения предмета. Сущность 2-го этапа определения критерия оценки по учебной дисциплине заключается в определении подхода к оцениванию на основе ранее полученных данных о сформированности каждой компетенции, обязательной к выработке в процессе изучения предмета. В качестве основного критерия при оценке обучаемого при определении уровня освоения учебной дисциплины наличие сформированных у него компетенций по результатам освоения учебной дисциплины.

Положительная оценка по дисциплине, может выставляться и при не полной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.

## Шкала оценивания сформированности компетенции в рамках дисциплины

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Уровень освоения дисциплины, при котором у обучаемого не сформировано более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции</p>	<p>При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность до-формирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно»</p>	<p>Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо».</p>	<p>Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90% сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций</p>



### **7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в производственной э преддипломной практики**

#### **7.3.1 Вопросы для текущего контроля.**

**Целью устного опроса** является закрепление, углубление и систематизация знаний студентов, полученных в процессе прохождения и при самостоятельной работе; проведение устного опроса позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

#### **Проверяемые компетенции:**

Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)

Способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)

Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)

Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)

Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)

Способностью проводить анализ исходных данных для проектирования

подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)

Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)

Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)

Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)

Способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)

Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)

Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)

Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики (ПКУ-1)

1. Описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие.
2. Определить виды информации ограниченного доступа, обрабатываемые предприятием.
3. Ознакомиться с формами организации производственного процесса и его технологическим обеспечением.
4. Выявить угрозы безопасности предприятия.
5. Проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности.
6. Изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации.
7. Изучить методы и средства защиты информации, применяемые на предприятии.
8. Изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта.
9. Разработать модель угроз для конкретной информационной системы предприятия.
10. Изучить основные обязанности должностных лиц в области защиты информации.
11. Проанализировать методы контроля в области защиты информации, используемые в организации.
12. Разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия.
13. Предложить перечень мероприятий по улучшению системы защиты информации на предприятии.
14. Оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности.

15. Провести анализ безопасности программных продуктов, используемых на предприятии.
16. Изучить возможные методы прогнозирования появления уязвимостей в программном коде.
17. Произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД.
18. Изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации.
19. Спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения.
20. Спроектировать систему физической защиты информации.
21. Разработать политику информационной безопасности предприятия.
22. Проанализировать систему компьютерной безопасности предприятия.
23. Изучить систему контроля и управления доступом предприятия.
24. Ознакомиться с системой защиты персональных данных в организации.
25. Изучить виды правонарушений при совершении компьютерных преступлений.

### **7.3.2. Промежуточный контроль по практике**

Промежуточный контроль осуществляется в виде устного отчета о результатах прохождения производственной преддипломной практики.

К промежуточному контролю допускаются студенты

- правильно заполнившие дневник производственной преддипломной практики;
- получившие положительный отзыв руководителя практики.

### **7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций**

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций по производственной преддипломной практике проводится в форме

текущей и промежуточной аттестации.

Контроль текущей успеваемости обучающихся - текущая аттестация - проводится в процессе прохождения практики с целью определения уровня усвоения обучающимися знаний; формирования у них умений и навыков; своевременного выявления преподавателем недостатков в подготовке студентов и принятия необходимых мер по ее корректировке; совершенствованию методики обучения; организации учебной работы и оказания обучающимся индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:

- на занятиях (опрос);
- по результатам проверки качества материалов, собранных учащимися в ходе практики.

Промежуточная аттестация по практике проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков по производственной эксплуатационной практике требованиям ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» в форме зачета.

Зачет проводится после завершения практики в объеме рабочей учебной программы. Форма проведения зачета определяется учебно-методическим советом института (путем собеседования по вопросам; письменная работа, тестирование и др.). Оценка по результатам зачета - «зачтено», «незачтено».

«Зачтено» ставится, если задания на практику выполнено в полном объёме, получен положительный отзыв руководителя практики, студент предоставил все необходимые материалы, оформил дневник практики, показана совокупность осознанных знаний. Знание по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной практики с

использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи.

«Зачтено» также ставится, если задания на практику выполнено в полном объеме, получен положительный отзыв руководителя практики от организации-партнёра, студент предоставил все необходимые материалы, оформил дневник практики дал развернутые ответы на поставленные вопросы, показал умение выделить существенные и несущественные признаки, причинно-следственные связи, но допустил 2-3 неточности или незначительные ошибки. Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне.

«Незачтено» ставится в случае, когда задания на практику выполнено не в полном объеме, отзыв руководителя практики от организации-партнёра, отрицателен, или студент не предоставил всех необходимых материалов, не оформил по установленной форме дневник практики, или не показал в ходе собеседования совокупность осознанных знаний; присутствуют фрагментарность, нелогичность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента, или ответ на вопрос полностью отсутствует, или отказ от ответа. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения практики.

Все виды текущего контроля осуществляются в ходе решения производственных и иных задач.

Каждая форма контроля по дисциплине включает в себя теоретические вопросы, позволяющие оценить уровень освоения студентами знаний и практические задания, выявляющие степень сформированности умений и навыков.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки (на каждом занятии).
2. Многоступенчатость: оценка (как преподавателем, так и студентами группы) и самооценка обучающегося, обсуждение результатов и комплекса мер по устранению недостатков.
3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.
4. Соблюдение последовательности проведения оценки: предусмотрено, что развитие компетенций идет по возрастанию их уровней сложности, а оценочные средства на каждом этапе учитывают это возрастание.

Краткая характеристика процедуры реализации текущего и промежуточного контроля по дисциплине для оценки компетенций обучающихся представлена в таблице:

<b>№ п/п</b>	<b>Наименование оценочного средства</b>	<b>Краткая характеристика процедуры оценивания компетенций</b>	<b>Представление оценочного средства в фонде</b>
1	Проблемная задача	Совместная деятельность группы обучающихся и преподавателя под управлением преподавателя с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Примеры задач
2	Устный опрос	Устный опрос по основным терминам может проводиться в начале/конце практического занятия в течение 15-20 мин.	Вопросы по темам/разделам дисциплины

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

### **Основная литература**

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ [Т. А. Полякова [и др.] ; под ред.: Т. А. Поляковой, А. А. Стрельцова. - Москва: Юрайт, 2019. - 1 on-line, 325 с.: рис.. - (Бакалавр и магистр. Академический курс)
2. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/13931.html>

### **Дополнительная литература**

1. Мельников, В. П. Информационная безопасность [Электронный ресурс]: [учеб. пособие]/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 8-е изд., испр.. - Москва: Академия, 2013. - 1 эл. опт. диск (CD-ROM), 336 с.: рис., табл.). - - Библиогр.: с. 327-328 (37 назв.)
2. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие для вузов/ Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР; Москва: Инфра-М, 2017. - 202, [1] с.: ил. - (Высшее образование). - Библиогр.: с. 195-198. - ISBN 978-5-369-01603-9. - ISBN 978-5-16-012372-1: 485.89, 485.89, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
3. Сагдеев, К. М. Физические основы защиты информации: учеб. пособие для вузов/ К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. - 2-е изд., испр. и доп.. - Санкт-Петербург: Интермедия, 2017. - 408 с.: ил. - Библиография: с. 405-406 (22 названия). - ISBN 978-5-4383-0141-7: 780.00, 780.00, р.



- Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
4. Рагозин, Ю. Н. Инженерно-техническая защита информации: учеб. пособие по физ. основам образования техн. каналов утечки информации по практикуму оценки их опасности/ Ю. Н. Рагозин. - Санкт-Петербург: Интермедия, 2018. - 165 с.: ил.. - Библиогр.: с. 164-165 (31 назв.). - ISBN 978-5-4383-0161-5: 680.00, 680.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г. А. Бузов. - Москва: Горячая линия-Телеком, 2014. - 585, [4] л. вкл. с.: ил.. - Библиогр.: с. 574-581 (126 назв.). - ISBN 978-5-9912-0424-8: 712.80, 712.80, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  6. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации/ В. Я. Ищейнов, М. В. Мещатунян. - 2-е изд., перераб. и доп.. - Москва: Форум; Москва: ИНФРА-М, 2014. - 255 с. - (Высшее образование - бакалавриат). - Библиогр.: с. 251-253. - ISBN 978-5-91134-856-4. - ISBN 978-5-16-009578-3: 349.69, 349.69, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  7. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации/ Г. А. Бузов. - М.: Горячая линия-Телеком, 2013. - 239 с.: ил. - Библиогр.: с. 230-235. - ISBN 978-5-9912-0121-6: 303.60, 303.60, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  8. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 608-609 (34 назв.). - ISBN 978-5-9912-0084-4: 699.60, 699.60, р. Имеются экземпляры в отделах /There are copies in departments: всего

/all 15: УБ(14), ч.з.№3(1)

### Перечень интернет-источников

1. «Национальная электронная библиотека» (<http://xn--90ax2c.xn--p1ai/>).
2. ЭБС Кантиана (<https://elib.kantiana.ru/>).
3. ЭБС IPR BOOKS (<https://www.iprbookshop.ru/78574.html>).
4. ЭБС Znanium (<https://znanium.com/catalog/document?id=333215>).

### 9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

1. Использование системы электронного образовательного контента БФУ им. И. Канта <http://lms-3.kantiana.ru/>.
2. Использование электронной образовательной среды БФУ им. И. Канта <https://teams.microsoft.com/>

### 10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Лаборатория технических средств защиты информации Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, третий этаж, ауд. 315	Нелинейный локатор "Лорнет" Анализ спектра "СК-4 Белан-32" Антенна логопериодическая "ЕЛВ-26" Аппаратно-программный лабораторный комплекс средств защиты информации Анализатор проводных линий "ОТКЛИК" Аппаратно-программный комплекс защиты информации от несанкционированного доступа Программно-аппаратный комплекс "Навигатор-ПЗГ" АПКШ "Континент" Комплект специальных средств защиты информации от утечки по техническим каналам Программно-аппаратный комплекс автоматического обнаружения, идентификации и нейтрализации подслушивающих	Типовое программное обеспечение: Microsoft Windows 7 pro, Microsoft Office standart 2010 – договор №1980/12 14.12.2012 ООО "ЭСЭМДЖИ", акт АА-118 от 21.12.2012 Антивирусное программное обеспечение Kaspersky Endpoint Security договор № 1311/19 от 01.03.2019 ООО "СофтЛайн Проекты" акт Pr001333 от 25.07.2019
---	--	---

	<p>устройств "Крона"          Комплекс многофункциональных поисковых приборов локализации каналов утечки информации          Проектор Toshiba TDP-EX1 переносной          Электронные наборы/модули СС1020ЕМК-433 Т1          Инструментарий для модулей фирмы Т1/СС СС1070ЕМ-433 Т1          Инструментарий для модулей фирмы Т1/СС СС1070ЕМ-433 Т1          Инструментарий для модулей фирмы Т1/СС СС1070ЕМ-433 Т1          Инструментарий для модулей фирмы Т1/СС СС1070ЕМ-433 Т1          Паяльная станция-фен нагретым воздухом          Осциллограф генератор PCSGU 250 usb          Комплект оборудования для экспериментального стенда микропроцессорной техники          Телевизор LG 42LW650S          Персональный компьютер с параметрами - Intel Core I3-3220, 3.3 GHz, 4Gb RAM, 1 Tb HDD, 21,5", keyboard, Mouse, LAN, Internet access</p>	
<p>Учебная лаборатория для самостоятельной работы, для работы над курсовыми и дипломными проектами          Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, четвертый этаж, ауд. 417</p>	<p>Телевизор LG 50LN540V          Рабочие станции DEPO Race G540S (7 шт.);          Мониторы 27" ViewSonic VX2739WM (7 шт.);          Цветной лазерный принтер формата А3 Hewlett-Packard Color LaserJet Enterprise CP5525dn;          Источники бесперебойного питания Mustek PowerMust 1590 (7 шт.);          Цветной плоттер формата А1 Hewlett-Packard HP Designjet T790;</p>	<p>Общесистемное программное обеспечение Microsoft Windows 7,          Общесистемное программное обеспечение Microsoft Office Standart 2010 – Договор поставки № 952 от 19.10.2011 ООО «Джи-Кей Системс»</p>



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
**ФГАОУ ВО «БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА»**  
ИНСТИТУТ ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК И  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**ДНЕВНИК  
ПРОИЗВОДСТВЕННОЙ ПРЕДДИПЛОМНОЙ ПРАКТИКИ**

*Студента 4 курса*

*Направления подготовки 10.03.01 «Информационная безопасность»*

*Профиль подготовки «Организация и технология защиты информации»*

*Иванова Ивана Ивановича*

Калининград

20\_\_ год

1. Фамилия *Иванов*
2. Имя и отчество *Иван Иванович*
3. Курс 4
4. Направление подготовки 10.03.01 «Информационная безопасность»,  
Профиль подготовки «Организация и технология защиты информации»
5. Место прохождения практики \_\_\_\_\_  
\_\_\_\_\_
6. Срок практики \_\_.\_\_.20\_\_-\_\_.\_\_.20\_\_
7. Руководитель практики от института физико-математических наук и  
информационных технологий \_\_\_\_\_ / \_\_\_\_\_  
«\_\_» \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП \_\_\_\_\_ Бурмистров В. И.

печать

### *Даты прохождения практики*

Прибыл на место практики «\_\_» \_\_\_\_\_ 20\_\_ г

Назначен \_\_\_\_\_ практикантом  
Рабочее место, должность

Откомандирован в БФУ им. И. Канта «\_\_» \_\_\_\_\_ 20\_\_ г

Первый заместитель директора ИФМНиИТ

\_\_\_\_\_ Шпилевой А. А.  
подпись и печать

## ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

«СОГЛАСОВАНО»

Руководитель практики от БФУ им. И. Канта

«УТВЕРЖДАЮ»

Научный руководитель

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

для \_\_\_\_\_,  
*(ФИО студента)*

**Место прохождения:** институт физико-математических наук и информационных технологий  
БФУ им. И. Канта

**Срок прохождения:** с «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_ г.

**Цель прохождения:** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**Задачи:** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### Содержание:

1	Подготовительный этап	Ознакомление с программой практики
		Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации
2	Основной этап	Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка
		...
		...
3	Заключительный этап	Сбор материалов для дневника практики.
		Оформление дневника практики в электронном и печатном виде

### Планируемые результаты:

1	
2	
3	
4	
5	
...	

**Форма отчетности:** \_\_\_\_\_

**Форма контроля:** \_\_\_\_\_

Ознакомлен(а) \_\_\_\_\_  
*(подпись студента)*

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.



				Выходной		
__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__
				Выходной		
__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__
				Выходной		
__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__
				Выходной	Сбор материалов для дневника практики.	Оформление дневника практики в электронном и печатном виде.



***Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.***

Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка проведен \_\_.\_\_.20\_\_ г.

С требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка ознакомлен \_\_.\_\_.20\_\_ г.

\_\_\_\_\_ / \_\_\_\_\_

Подпись ответственного за проведение инструктажей

\_\_\_\_\_ / \_\_\_\_\_  
подпись и печать

### *Повседневный план производственной преддипломной практики*

<i>Дата</i>	<i>Выполненные работы</i>	<i>Подпись руководителя практики</i>
__ . __ . 20 __	Ознакомление с программой практики. Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации. Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.	
__ . __ . 20 __	<i>Подробное описание видов работ</i>	
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		

__..20__		
__..20__		
__..20__		
__..20__		
__..20__		
__..20__		Выходной
__..20__	Сбор материалов для дневника практики.	
__..20__	Оформление дневника практики в электронном и печатном виде.	

**Список материалов,  
собранных студентом в период прохождения практики**

№ п/п	
1.	
2.	
3.	
4.	
5.	
6.	





## **ПРИЛОЖЕНИЕ**

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА**

**Институт физико-математических наук и информационных технологий**

«Согласовано»

Ведущий менеджер ООП ИФМНИИТ  
В.И.Бурмистров

«10» марта 2020 г.

«Утверждено»  
Директор ИФМНИИТ

А.В.Юров

«10» марта 2020 г.



**ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРОЕКТНО-  
ТЕХНОЛОГИЧЕСКОЙ ПРАКТИКИ**

для студентов 4 курса  
очной формы обучения

направления подготовки 10.03.01.

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

профиль подготовки **«ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ  
ИНФОРМАЦИИ»**

уровень высшего образования – бакалавриат

Калининград, 2020 г.



## Лист согласования

**Составители:** доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

Программа обсуждена и утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий.

Протокол № \_\_\_/\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Председатель учебно-методического совета \_\_\_\_\_ первый  
заместитель директора института, к.ф.-м.н., доцент, Шпилевой А. А.

Программа пересмотрена на заседании учебно-методического совета института физико-математических наук и информационных технологий. Внесены следующие изменения (или изменений не внесено) \_\_\_\_\_

Протокол № \_\_\_\_\_ от « \_\_\_ » \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП \_\_\_\_\_ Бурмистров В. И.

СОДЕРЖАНИЕ  
ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРОЕКТНО-  
ТЕХНОЛОГИЧЕСКОЙ ПРАКТИКИ

1. Указание вида практики, способа и формы ее проведения.....	4
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.....	4
3. Указание места практики в структуре образовательной программы.....	9
4. Указание объема практики в зачетных единицах и ее продолжительности в неделях и академических часах.....	11
5. Содержание практики.....	12
6. Указание форм отчетности по практике.....	13
7. Фонд оценочных средств проведения промежуточной аттестации обучающихся по практике.....	13
7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках производственной технологической практики.....	13
7.2 Показатели и критерии оценивания компетенций на различных этапах их формирования.....	17
7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в рамках производственной технологической практики.....	22
7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.....	24
8. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики.....	27
9. Перечень информационных технологий, используемых при проведении практики.....	29
10. Описание материально-технической базы, необходимой для проведения практики.....	30
Приложение 1.....	32

## **1. УКАЗАНИЕ ВИДА ПРАКТИКИ, СПОСОБА И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ**

**Вид практики:** производственная практика.

**Способ проведения** производственной практики: стационарная.

Стационарная практика проводится в образовательной организации, в которой обучающиеся осваивают образовательную программу, или в иных организациях, с которыми действуют соответствующие договорные отношения.

**Формы проведения** производственной практики: невыездная, непрерывная. Организация проведения производственной практики осуществляется путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения практики.

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

**Цели производственной проектно-технологической практики:**

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла базовой и вариативной частей, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;
- изучение информационной структуры предприятия, как объекта информатизации;
- изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;
- формирование навыков самостоятельного решения поставленных производственных задач;
- выбор темы выпускной квалификационной работы и ее выполнение.

**К основным задачам производственной проектно-технологической**

**практики** относятся:

- закрепление и расширение теоретических и практических знаний;
- развитие профессиональных навыков и навыков деловой коммуникации;
- сбор необходимых материалов для написания отчета по практике;
- проведение анализа и обобщения результаты собственных исследований;
- получение практических данных, для написания выпускной квалификационной работы, приобретения навыков их обработки.

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Результаты освоения ООП	Перечень планируемых результатов обучения по дисциплине
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	<b>Знать:</b> архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры; принципы построения и работы ПЭВМ <b>Уметь:</b> определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач <b>Владеть:</b> навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих	<b>Знать:</b> принципы метрологического обеспечения, стандартизации и сертификации; способы и приёмы наладки, настройки, регулировки и испытания оборудования,

	<p>нормативных и методических документов</p>	<p>тестирование, настройка и обслуживание аппаратно-программных средств;  методы и способы проведения всех видов измерений параметров оборудования и сквозных каналов и трактов (настроечных, приёмодаточных, эксплуатационных и аварийных);  принципы оформления и делопроизводства в области метрологического обеспечения, стандартизации и сертификации телекоммуникаций</p> <p><b>Уметь:</b>  самостоятельно работать на компьютере и в компьютерных сетях, моделировать на компьютере устройства, системы и процессы с использованием универсальных пакетов прикладных компьютерных программ;  применять принципы метрологического обеспечения и способы инструментальных измерений, используемых в области инфокоммуникационных технологий и систем связи;  организовать и осуществить проверку технического состояния и ресурса оборудования; применять современные методы их обслуживания и ремонта</p> <p><b>Владеть:</b>  основными приёмами технической эксплуатации и метрологического обеспечения аппаратуры и систем телекоммуникаций</p>
--	--	---

### 3. УКАЗАНИЕ МЕСТА ПРОИЗВОДСТВЕННОЙ ПРОЕКТНО-ТЕХНОЛОГИЧЕСКОЙ ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Производственная проектно-технологическая практика представляет собой дисциплину вариативной части (Б2.В.02(П)) блока Б2 «Практика» подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность» по профилю подготовки «Организация и технология защиты информации».

Логическая и содержательная связь дисциплин, участвующих в формировании представленных в п.1 компетенций, содержится в ниже представленной таблице:

<b>Код компетенции</b>	<b>Предшествующие дисциплины</b>	<b>Данная дисциплина</b>	<b>Последующие дисциплины</b>
ПК-7	<p>Организационное и правовое обеспечение информационной безопасности</p> <p>Информационная безопасность корпоративных сетей</p> <p>Защита персональных данных в организации</p> <p>Аудит информационной безопасности автоматизированных систем</p> <p>Криптографические протоколы</p> <p>Защита информации в кредитно-финансовых организациях</p> <p>Производственная эксплуатационная практика</p>	<p>Производственная технологическая практика</p>	<p>Защита программ и данных</p> <p>Основы построения защищенных баз данных</p> <p>Криптографические протоколы для защиты банковской информации</p> <p>Надежность, эргономика и качество информационных систем</p> <p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p>
ПК-8	<p>Основы управления информационной безопасности</p> <p>Организационное и правовое обеспечение информационной безопасности</p> <p>Метрология, стандартизация и сертификация</p> <p>Учебная практика по получению первичных профессиональных умений и навыков</p> <p>Производственная эксплуатационная практика</p>		<p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p> <p>Астрономия и астрофизика</p> <p>Космология</p>

#### **4. УКАЗАНИЕ ОБЪЕМА ПРАКТИКИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТИ В НЕДЕЛЯХ И АКАДЕМИЧЕСКИХ ЧАСАХ.**

Производственная проектно-технологическая практика проводится в 7-м учебном семестре в течение 2 недель. Трудоемкость учебной практики - 3

зачетные единицы (ЗЕ) и 108 академических часа.

## 5. СОДЕРЖАНИЕ ПРАКТИКИ

№ п/п	Этапы практики	Виды работы	Трудоёмкость, час.
1	Подготовительный (ознакомительный) этап	Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации, прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка. Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики	4
2	Основной этап	Ознакомление с деятельностью предприятия. Определение методов и средств защиты информации, используемых на предприятии. Выполнение практических заданий. Сбор материалов для отчетной документации, обработка и систематизация фактического и литературного материала; наблюдения; измерения и другие, выполняемые обучающимся самостоятельно виды работ.	88
3	Заключительный этап	Подготовка отчетной документации, получение характеристики о работе и (или) характеристики – отзыва руководителя практики от университета, представление отчетной документации	16
<b>Итого 3 З.Е.</b>			<b>108</b>
* ЗЕ -зачетная единица			

## **6. УКАЗАНИЕ ФОРМ ОТЧЕТНОСТИ ПО ПРАКТИКЕ**

Студент выполняет программу производственной проектно-технологической практики в соответствии с планом-графиком практики и индивидуальным заданием на практику, утверждаемым учебно-методическим советом института, ведет дневник практики, который защищает после окончания практики. В зависимости от специализации подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Для текущего контроля посещаемости производственной проектно-технологической практики используется стандартный журнал посещения занятий, который будет вести руководитель практики.

Отчет о результатах прохождения производственной проектно-технологической практики заслушивается на заседании учебно-методического совета института.

Дневник производственной проектно-технологической практики представлен в Приложении 1.

## **7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ**

### **7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках производственной технологической практики**

Контролируемые модули, разделы (темы) практики	Индекс контролируемой компетенции (или её части)	Содержание компетенции	Оценочные средства по этапам формирования компетенций	
			Текущий контроль по практике	промежуточный контроль по практике



<p>Подготовительный (ознакомительный) этап Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации, прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка. Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики</p>	<p>ПК-7</p>	<p>Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p>	<p>Устный опрос</p>	
<p>Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации, прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка. Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики</p>	<p>ПК-8</p>	<p>Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p>	<p>Устный опрос</p>	

<p>Основной этап</p> <p>Ознакомление с деятельностью предприятия.</p> <p>Определение методов и средств защиты информации, используемых на предприятии.</p> <p>Выполнение практических заданий.</p> <p>Сбор материалов для отчетной документации, обработка и систематизация фактического и литературного материала; наблюдения; измерения и другие, выполняемые обучающимся самостоятельно виды работ.</p>	ПК-7	Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос	
	ПК-8	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос	
<p>Заключительный этап</p> <p>Подготовка отчетной документации, получение характеристики о работе и (или) характеристики – отзыва руководителя практики от университета, представление отчетной документации</p>	ПК-7	Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос	
	ПК-8	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос	
				зачет

**Этапы формирования компетенций в процессе освоения образовательной программы в рамках производственной проектно-технологической практики**

Индекс контролируемой компетенции	№ Учебной недели № Темы раздела дисциплины/модуля			
	16	16	17	17
	1	2	2	3
	Этапы формирования компетенции			
ПК-7	+	+	+	+
ПК-8	+	+	+	+

**7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования**  
**Критерии определения сформированности компетенций на различных этапах их формирования**

Показатели	ниже порогового	пороговый	достаточный	повышенный
<b>Критерии</b>	Компетенция не сформирована. Студент не способен определить основные понятия, воспроизвести основные факты, идеи теории информационной безопасности, не знает основные методы решения типовых задач. Не умеет работать со справочной литературой, не способен представить результаты своей работы. Не владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, не способен применять информационные технологии для решения типовых задач	Компетенция сформирована на «удовлетворительно». Студент дает определения основных понятий, воспроизводит основные факты, идеи, теории информационной безопасности, знает основные методы решения типовых задач. Умеет работать со справочной литературой, представлять результаты своей работы. Владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, способен применять информационные технологии для решения типовых задач	Компетенция сформирована на «хорошо». Студент понимает связи между различными понятиями теории, аргументирует выбор метода решения задачи и умеет их применять на практике. Применяет методы решения задач в незнакомых ситуациях, умеет корректно выражать и аргументированно обосновывать положения предметной области знания. Способен применять информационные технологии для решения прикладных задач, адаптировать типовые технологии к решению практико-ориентированных задач.	Компетенция сформирована «отлично». Студент устанавливает связи между основными концепциями в предметной области, теориями дисциплинами. Оценивает достоверность полученного решения задачи, методы решения задачи и выбирает оптимальный метод, разрабатывает модели реальных процессов и ситуаций. Способен передавать результат проведенных исследований в виде конкретных рекомендаций в терминах предметной области знания, интерпретировать знания предметной области.

Поскольку практически всякая учебная дисциплина призвана формировать сразу несколько компетенций, критерии оценки целесообразно формировать в два этапа.

1-й этап: определение критериев оценки отдельно по каждой формируемой компетенции. Сущность 1-го этапа состоит в определении шкал оценивания для оценивания отдельно взятой компетенции на основе продемонстрированного обучаемым уровня самостоятельности в применении полученных в ходе изучения учебной дисциплины, знаний, умений и навыков.

## Шкала оценивания компетенций

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины</p>	<p>Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне</p>	<p>Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке</p>	<p>Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи</p>

2-й этап: определение критериев для оценки уровня обученности по учебной дисциплине на основе комплексного подхода к уровню сформированности всех компетенций, обязательных к формированию в процессе изучения предмета. Сущность 2-го этапа определения критерия оценки по учебной дисциплине заключается в определении подхода к оцениванию на основе ранее полученных данных о сформированности каждой компетенции, обязательной к выработке в процессе изучения предмета. В качестве основного критерия при оценке обучаемого при определении уровня освоения учебной дисциплины наличие сформированных у него компетенций по результатам освоения учебной дисциплины.

Положительная оценка по дисциплине, может выставляться и при не полной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.

## Шкала оценивания сформированности компетенции в рамках дисциплины

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Уровень освоения дисциплины, при котором у обучаемого не сформировано более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции</p>	<p>При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность до-формирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно»</p>	<p>Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо».</p>	<p>Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90% сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций</p>



### **7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в производственной проектно-технологической практики**

#### **7.3.1 Вопросы для текущего контроля.**

**Целью устного опроса** является закрепление, углубление и систематизация знаний студентов, полученных в процессе прохождения и при самостоятельной работе; проведение устного опроса позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

#### **Проверяемые компетенции:**

**ПК-7:** Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

**ПК-8:** Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

1. Определить виды информации ограниченного доступа, обрабатываемые предприятием.
2. Выявить угрозы безопасности предприятия.
3. Изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации.
4. Изучить методы и средства защиты информации, применяемые на предприятии; изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта.

5. Разработать модель угроз для конкретной информационной системы предприятия.
6. Проанализировать методы контроля в области защиты информации, используемые в организации.
7. Оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности.
8. Изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации.
9. Разработать политику информационной безопасности предприятия.
10. Изучить систему контроля и управления доступом предприятия.
11. Провести анализ рисков информационной безопасности.
12. Разработать программное решение для обеспечения информационной безопасности.
13. Исследовать проблемы безопасности при использовании мобильных устройств.
14. Изучить обеспечение информационной безопасности при использовании СЭД.

### **7.3.2. Промежуточный контроль по практике**

Промежуточный контроль осуществляется в виде устного отчета о результатах прохождения производственной технологической практики.

К промежуточному контролю допускаются студенты

- правильно заполнившие дневник производственной технологической практики;
- получившие положительный отзыв руководителя практики.

## **7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций**

Оценка знаний, умений, навыков, характеризующая этапы формирования

компетенций по производственной проектно-технологической практике проводится в форме текущей и промежуточной аттестации.

Контроль текущей успеваемости обучающихся - текущая аттестация - проводится в процессе прохождения практики с целью определения уровня усвоения обучающимися знаний; формирования у них умений и навыков; своевременного выявления преподавателем недостатков в подготовке студентов и принятия необходимых мер по ее корректировке; совершенствованию методики обучения; организации учебной работы и оказания обучающимся индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:

- на занятиях (опрос);
- по результатам проверки качества материалов, собранных учащимися в ходе практики.

Промежуточная аттестация по практике проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков по производственной эксплуатационной практике требованиям ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» в форме зачета.

Зачет проводится после завершения практики в объеме рабочей учебной программы. Форма проведения зачета определяется учебно-методическим советом института (путем собеседования по вопросам; письменная работа, тестирование и др.). Оценка по результатам зачета - «зачтено», «незачтено».

«Зачтено» ставится, если задания на практику выполнено в полном объёме, получен положительный отзыв руководителя практики, студент предоставил все необходимые материалы, оформил дневник практики, показана совокупность осознанных знаний. Знание по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения

неизвестных или нестандартных заданий в рамках учебной практики с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи.

«Зачтено» также ставится, если задания на практику выполнено в полном объеме, получен положительный отзыв руководителя практики от организации-партнёра, студент предоставил все необходимые материалы, оформил дневник практики дал развернутые ответы на поставленные вопросы, показал умение выделить существенные и несущественные признаки, причинно-следственные связи, но допустил 2-3 неточности или незначительные ошибки. Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне.

«Незачтено» ставится в случае, когда задания на практику выполнено не в полном объеме, отзыв руководителя практики от организации-партнёра, отрицателен, или студент не предоставил всех необходимых материалов, не оформил по установленной форме дневник практики, или не показал в ходе собеседования совокупность осознанных знаний; присутствуют фрагментарность, нелогичность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента, или ответ на вопрос полностью отсутствует, или отказ от ответа. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения практики.

Все виды текущего контроля осуществляются в ходе решения

производственных и иных задач.

Каждая форма контроля по дисциплине включает в себя теоретические вопросы, позволяющие оценить уровень освоения студентами знаний и практические задания, выявляющие степень сформированности умений и навыков.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки (на каждом занятии).
2. Многоступенчатость: оценка (как преподавателем, так и студентами группы) и самооценка обучающегося, обсуждение результатов и комплекса мер по устранению недостатков.
3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.
4. Соблюдение последовательности проведения оценки: предусмотрено, что развитие компетенций идет по возрастанию их уровней сложности, а оценочные средства на каждом этапе учитывают это возрастание.

Краткая характеристика процедуры реализации текущего и промежуточного контроля по дисциплине для оценки компетенций обучающихся представлена в таблице:

№ п/п	Наименование оценочного средства	Краткая характеристика процедуры оценивания компетенций	Представление оценочного средства в фонде
1	Устный опрос	Устный опрос по основным терминам может проводиться в начале/конце практического занятия в течение 15-20 мин.	Вопросы по темам/разделам дисциплины

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

### **Основная литература**

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ [Т. А. Полякова [и др.] ; под ред.: Т. А. Поляковой, А. А.

- Стрельцова. - Москва: Юрайт, 2019. - 1 on-line, 325 с.: рис.. - (Бакалавр и магистр. Академический курс)
2. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/13931.html>

### Дополнительная литература

1. Мельников, В. П. Информационная безопасность [Электронный ресурс]: [учеб. пособие]/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 8-е изд., испр.. - Москва: Академия, 2013. - 1 эл. опт. диск (CD-ROM), 336 с.: рис., табл.). - - Библиогр.: с. 327-328 (37 назв.)
2. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие для вузов/ Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР; Москва: Инфра-М, 2017. - 202, [1] с.: ил. - (Высшее образование). - Библиогр.: с. 195-198. - ISBN 978-5-369-01603-9. - ISBN 978-5-16-012372-1: 485.89, 485.89, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
3. Сагдеев, К. М. Физические основы защиты информации: учеб. пособие для вузов/ К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. - 2-е изд., испр. и доп.. - Санкт-Петербург: Интермедия, 2017. - 408 с.: ил. - Библиография: с. 405-406 (22 названия). - ISBN 978-5-4383-0141-7: 780.00, 780.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
4. Рагозин, Ю. Н. Инженерно-техническая защита информации: учеб. пособие по физ. основам образования техн. каналов утечки информации по практикуму оценки их опасности/ Ю. Н. Рагозин. - Санкт-Петербург: Интермедия, 2018. - 165 с.: ил.. - Библиогр.: с. 164-165 (31 назв.). - ISBN 978-5-4383-0161-5: 680.00, 680.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)

5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г. А. Бузов. - Москва: Горячая линия-Телеком, 2014. - 585, [4] л. вкл. с.: ил.. - Библиогр.: с. 574-581 (126 назв.). - ISBN 978-5-9912-0424-8: 712.80, 712.80, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
6. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации/ В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп.. - Москва: Форум; Москва: ИНФРА-М, 2014. - 255 с. - (Высшее образование - бакалавриат). - Библиогр.: с. 251-253. - ISBN 978-5-91134-856-4. - ISBN 978-5-16-009578-3: 349.69, 349.69, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
7. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации/ Г. А. Бузов. - М.: Горячая линия-Телеком, 2013. - 239 с.: ил. - Библиогр.: с. 230-235. - ISBN 978-5-9912-0121-6: 303.60, 303.60, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
8. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 608-609 (34 назв.). - ISBN 978-5-9912-0084-4: 699.60, 699.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(14), ч.з.N3(1)

#### **Перечень интернет-источников**

1. «Национальная электронная библиотека» (<http://xn--90ax2c.xn--p1ai/>).
2. ЭБС Кантиана (<https://elib.kantiana.ru/>).
3. ЭБС IPR BOOKS (<https://www.iprbookshop.ru/78574.html>).
4. ЭБС Znanium (<https://znanium.com/catalog/document?id=333215>).

## 9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

1. Использование системы электронного образовательного контента БФУ им. И. Канта <http://lms-3.kantiana.ru/>.
2. Использование электронной образовательной среды БФУ им. И. Канта <https://teams.microsoft.com/>

## 10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

<p>Лаборатория технических средств защиты информации Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, третий этаж, ауд. 315</p>	<p>Нелинейный локатор "Лорнет" Анализ спектра "СК-4 Белан-32" Антенна логопериодическая "ЕЛВ-26" Аппаратно-программный лабораторный комплекс средств защиты информации Анализатор проводных линий "ОТКЛИК" Аппаратно-программный комплекс защиты информации от несанкционированного доступа Программно-аппаратный комплекс "Навигатор-ПЗГ" АПКШ "Континент" Комплект специальных средств защиты информации от утечки по техническим каналам Программно-аппаратный комплекс автоматического обнаружения, идентификации и нейтрализации подслушивающих устройств "Крона" Комплекс многофункциональных поисковых приборов локализации каналов утечки информации Проектор Toshiba TDP-EX1 переносной Электронные наборы/модули СС1020ЕМК-433 Т1 Инструментарий для модулей фирмы Т1/СС СС1070ЕМ-433 Т1 Инструментарий для модулей</p>	<p>Типовое программное обеспечение: Microsoft Windows 7 pro, Microsoft Office standart 2010 – договор №1980/12 14.12.2012 ООО "ЭСЭМДЖИ", акт АА-118 от 21.12.2012 Антивирусное программное обеспечение Kaspersky Endpoint Security договор № 1311/19 от 01.03.2019 ООО "СофтЛайн Проекты" акт Pr001333 от 25.07.2019</p>
--	---	--



	<p>фирмы TI/CC CC1070EM-433 TI  Инструментарий для модулей  фирмы TI/CC CC1070EM-433 TI  Инструментарий для модулей  фирмы TI/CC CC1070EM-433 TI  Паяльная станция-фен нагретым  воздухом  Осциллограф генератор PCSGU  250 usb  Комплект оборудования для  экспериментального стенда  микропроцессорной техники  Телевизор LG 42LW650S  Персональный компьютер с  параметрами - Intel Core I3-3220,  3.3 GHz, 4Gb RAM, 1 Tb HDD,  21,5”, keyboard,. Mouse, LAN,  Internet access</p>	
<p>Учебная лаборатория для  самостоятельной работы,  для работы над  курсовыми и дипломными  проектами  Россия, 236016,  Калининградская обл., г.  Калининград, ул. А.  Невского, дом № 14,  корпус №2, четвертый  этаж, ауд. 417</p>	<p>Телевизор LG 50LN540V  Рабочие станции DEPO Race  G540S (7 шт.);  Мониторы 27" ViewSonic  VX2739WM (7 шт.);  Цветной лазерный принтер  формата А3 Hewlett-Packard  Color LaserJet Enterprise  CP5525dn;  Источники бесперебойного  питания Mustek PowerMust 1590  (7 шт.);  Цветной плоттер формата А1  Hewlett-Packard HP Designjet  T790;</p>	<p>Общесистемное программное  обеспечение Microsoft Windows  7,  Общесистемное программное  обеспечение Microsoft Office  Standart 2010 – Договор  поставки № 952 от 19.10.2011  ООО «Джи-Кей Системс»</p>



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ФГАОУ ВО «БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА»  
ИНСТИТУТ ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК И  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**ДНЕВНИК  
ПРОИЗВОДСТВЕННОЙ ПРОЕКТНО-ТЕХНОЛОГИЧЕСКОЙ  
ПРАКТИКИ**

*Студента 4 курса*

*Направления подготовки 10.03.01 «Информационная безопасность»*

*Профиль подготовки «Организация и технология защиты информации»*

*Иванова Ивана Ивановича*

Калининград

20\_\_ год

1. Фамилия *Иванов*
2. Имя и отчество *Иван Иванович*
3. Курс 3
4. Направление подготовки 10.03.01 «Информационная безопасность»,  
Профиль подготовки «Организация и технология защиты информации»
5. Место прохождения практики \_\_\_\_\_  
\_\_\_\_\_
6. Срок практики \_\_.\_\_.\_\_\_\_-\_\_.\_\_.\_\_\_\_
7. Руководитель практики от института физико-математических наук и информационных технологий \_\_\_\_\_ / \_\_\_\_\_  
«\_\_» \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП \_\_\_\_\_ Бурмистров В. И.

печать

### *Даты прохождения практики*

Прибыл на место практики «\_\_» \_\_\_\_\_ 20\_\_ г

Назначен \_\_\_\_\_ практикантом  
Рабочее место, должность

Откомандирован в БФУ им. И. Канта «\_\_» \_\_\_\_\_ 20\_\_ г

Первый заместитель директора ИФМНиИТ

\_\_\_\_\_ Шпилевой А. А.  
подпись и печать

## ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

«УТВЕРЖДАЮ»

Руководитель практики от БФУ им. И. Канта

\_\_\_\_\_ / \_\_\_\_\_ /  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

для \_\_\_\_\_,  
(ФИО студента)

Место прохождения: \_\_\_\_\_

Срок прохождения: с «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_.

Цель прохождения: \_\_\_\_\_

Задачи: \_\_\_\_\_

### Содержание:

1	Подготовительный этап	Ознакомление с программой практики
		Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации
2	Основной этап	Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка
		...
		...
3	Заключительный этап	Сбор материалов для дневника практики.
		Оформление дневника практики в электронном и печатном виде

### Планируемые результаты:

1	
2	
3	
4	
5	
...	

Форма отчетности: \_\_\_\_\_

Форма контроля: \_\_\_\_\_

Ознакомлен(а) \_\_\_\_\_  
(подпись студента)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.



	Выходной					
__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__
	Выходной				Сбор материалов для дневника практики.	Оформление дневника практики в электронном и печатном виде.

***Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.***

Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка проведен \_\_.\_\_.20\_\_ г.

С требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка ознакомлен \_\_.\_\_.20\_\_ г.

\_\_\_\_\_ / \_\_\_\_\_

Подпись ответственного за проведение инструктажей

\_\_\_\_\_ / \_\_\_\_\_  
подпись и печать

**Повседневный план производственной проектно-технологической  
практики**

<i>Дата</i>	<i>Выполненные работы</i>	<i>Подпись руководителя практики</i>
__ . __ . 20 __	Ознакомление с программой практики. Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации. Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.	
__ . __ . 20 __		Выходной
__ . __ . 20 __	<i>Подробное описание видов работ</i>	
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __	Сбор материалов для дневника практики.	
__ . __ . 20 __	Оформление дневника практики в электронном и печатном виде.	



**Список материалов,  
собранных студентом в период прохождения практики**

№ п/п	
1.	
2.	
3.	
4.	
5.	
6.	





## **ПРИЛОЖЕНИЕ**

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА**

**Институт физико-математических наук и информационных технологий**

«Согласовано»

Ведущий менеджер ООП ИФМНиИТ  
В.И.Бурмистров

«10» марта 2020 г.

«Утверждено»  
Директор ИФМНиИТ

А.В.Юров

«10» марта 2020 г.



**ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ЭКСПЛУАТАЦИОННОЙ  
ПРАКТИКИ**

для студентов 3 курса  
очной формы обучения

направления подготовки 10.03.01.

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

профиль подготовки **«ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ  
ИНФОРМАЦИИ»**

уровень высшего образования – бакалавриат

Калининград, 2020 г.

## Лист согласования

**Составители:** доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

Программа обсуждена и утверждена на заседании учебно–методического совета института физико-математических наук и информационных технологий.

Протокол № \_\_\_/\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Председатель учебно-методического совета первый заместитель директора института, к.ф.-м.н., доцент, Шпилевой А. А.

Программа пересмотрена на заседании учебно-методического совета института физико-математических наук и информационных технологий. Внесены следующие изменения (или изменений не внесено) \_\_\_\_\_

Протокол № \_\_\_\_\_ от « \_\_\_ » \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП \_\_\_\_\_ Бурмистров В. И.

СОДЕРЖАНИЕ  
ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ЭКСПЛУАТАЦИОННОЙ  
ПРАКТИКИ

1. Указание вида практики, способа и формы ее проведения.....	4
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.....	4
3. Указание места практики в структуре образовательной программы.....	11
4. Указание объема практики в зачетных единицах и ее продолжительности в неделях и академических часах.....	16
5. Содержание практики.....	16
6. Указание форм отчетности по практике.....	17
7. Фонд оценочных средств проведения промежуточной аттестации обучающихся по практике.....	18
7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках производственной эксплуатационной практики.....	18
7.2 Показатели и критерии оценивания компетенций на различных этапах их формирования.....	25
7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в рамках производственной эксплуатационной практики.....	30
7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.....	33
8. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики.....	36
9. Перечень информационных технологий, используемых при проведении практики.....	38
10. Описание материально-технической базы, необходимой для проведения практики.....	39
Приложение 1.....	40

## **1. УКАЗАНИЕ ВИДА ПРАКТИКИ, СПОСОБА И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ**

**Вид практики:** производственная практика.

**Способ проведения** производственной практики: стационарная.

Стационарная практика проводится в образовательной организации, в которой обучающиеся осваивают образовательную программу, или в иных организациях, с которыми действуют соответствующие договорные отношения.

**Формы проведения** производственной практики: невыездная, непрерывная. Организация проведения производственной практики осуществляется путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения практики.

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

**Цели производственной эксплуатационной практики.** Закрепление, расширение, углубление и систематизация знаний, умений и навыков, полученных при изучении дисциплин профессионального цикла базовой и вариативной частей, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта. Производственная практика обеспечивает последовательность процесса формирования у студентов системы профессиональных компетенций в соответствии с профилем подготовки бакалавров, прививает студентам навыки самостоятельной работы по избранной профессии, дает возможность определения темы выпускной квалификационной работы и ее выполнения.

К основным задачам производственной эксплуатационной практики относятся:

- закрепление и расширение теоретических и практических знаний;



- развитие профессиональных навыков и навыков деловой коммуникации;
- изучение информационной структуры предприятия, как объекта информатизации;
- сбор необходимых материалов для написания отчета по практике;
- проведение анализа и обобщения результатов собственных исследований;
- получение практических данных, для написания выпускной квалификационной работы, приобретения навыков их обработки.

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Результаты освоения ООП	Перечень планируемых результатов обучения по дисциплине
ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	<p><b>Знать:</b>  об объектах информационной безопасности;  о направлениях защиты информации;  о требованиях к системам защиты информации</p> <p><b>Уметь:</b>  использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации</p> <p><b>Владеть:</b>  навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования</p>
ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности	<p><b>Знать:</b>  структуру системы управления информационной безопасностью;  приемы управлению информационной безопасностью  методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз</p> <p><b>Уметь:</b>  выделять процессы управления информационной безопасностью защищаемых объектов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью;  выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации;  обосновывать структуру системы управления</p>

		<p>информационной безопасностью в зависимости от характера угроз на объекте.</p> <p><b>Владеть:</b>  правилами, процедурами, практические приемы и пр. для управления информационной безопасности системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты методами и средствами минимизации угроз за счет совершенствования процессов управления</p>
ОПК-7	<p>Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	<p><b>Знать:</b>  основные понятия и теоремы теории информации и кодирования;  основные принципы и способы кодирования и декодирования;  характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования;  методы исследования кодов и их применений в ЭВМ и системах защиты информации.  основные классы кодов, их параметры и алгоритмы кодирования/декодирования  особенности различных подходов к организации информационного обеспечения  особенности научного исследования в области информатики и вычислительной техники, важнейшие методологические принципы научного исследования на базовом уровне</p> <p><b>Уметь:</b>  вычислять количество информации в сообщениях дискретного источника канала связи;  кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость;  оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования;  выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач  проектировать, оценивать и реализовывать информационное обеспечение информационных систем  осуществлять корректную постановку задачи исследования в области информатики и вычислительной техники на базовом уровне</p> <p><b>Владеть:</b></p>

		<p>основными методами кодирования и декодирования информации для различных задач</p> <p>средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом уровне</p>
ПК-1	<p>Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации</p>	<p><b>Знать:</b></p> <p>способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации;</p> <p><b>Уметь:</b></p> <p>классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения</p> <p><b>Владеть:</b></p> <p>навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>
ПК-2	<p>Способностью применять программные средства</p>	<p><b>Знать:</b></p> <p>основные категории требований к</p>

	<p>системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>	<p>программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий;</p> <p><b>Уметь:</b> определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий</p> <p><b>Владеть:</b> методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей</p>
ПК-3	<p>Способностью администрировать подсистемы информационной безопасности объекта защиты</p>	<p><b>Знать:</b> задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p><b>Уметь:</b> применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации;</p>

		<p>обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p><b>Владеть:</b>          средствами защиты информации в процессе хранения и передачи данных и методами их тестирования;          методикой определения эффективности предложенных решений с учетом снижения рисков</p>
ПК-4	<p>Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p><b>Знать:</b>          этапы и модели жизненного цикла информационных систем;          корпоративные стандарты и методики;          принципы хранения, защиты, передачи и получения информации в корпоративных сетях</p> <p><b>Уметь:</b>          разрабатывать структуру распределенных систем;          создавать клиент-серверные приложения для распределенных систем;          проектировать хранилища данных;          выполнять анализ корпоративных данных</p> <p><b>Владеть:</b>          навыками защиты информации в корпоративных сетях связи</p>
ПК-5	<p>Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации</p>	<p><b>Знать:</b>          правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;          правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;          основные отечественные и зарубежные стандарты в области компьютерной безопасности</p> <p><b>Уметь:</b>          применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности;          разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности;          разрабатывать предложения по совершенствованию системы управления</p>

		<p>информационной безопасностью компьютерных систем</p> <p><b>Владеть:</b>  навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках</p>
ПК-6	<p>Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p>	<p><b>Знать:</b>  методы анализа и оценки защищённости автоматизированных систем;  национальные и международные стандарты в области аудита и оценки информационной безопасности;  этапы и процедуры аудита информационной безопасности автоматизированных систем управления</p> <p><b>Уметь:</b>  разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем;  применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем;  применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы;  проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления</p> <p><b>Владеть:</b>  способами контроля эффективности реализации политики информационной безопасности организации;  анализом недостатков в функционировании системы защиты информации автоматизированной системы;  способами оценки защищённости автоматизированной системы;  методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации</p>

ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	<p><b>Знать:</b> архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры; принципы построения и работы ПЭВМ</p> <p><b>Уметь:</b> определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач</p> <p><b>Владеть:</b> навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования</p>
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	<p><b>Знать:</b> терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности в компьютерной сфере</p> <p><b>Уметь:</b> пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации</p> <p><b>Владеть:</b> навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках</p>

ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	<p><b>Знать:</b> направления создания правовой базы в области информационной безопасности; области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну</p> <p><b>Уметь:</b> разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов</p> <p><b>Владеть:</b> навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации</p>
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	<p><b>Знать:</b> основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности</p> <p><b>Уметь:</b> определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач</p> <p><b>Владеть:</b></p>



		<p>способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации;</p> <p>навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации</p>
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	<p><b>Знать:</b>  физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации;  основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности;</p> <p><b>Уметь:</b>  использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;  решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;  проводить классификацию экспериментов; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к</p>

		<p>практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач</p> <p><b>Владеть:</b>  навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну</p>
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	<p><b>Знать:</b>  основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации</p> <p><b>Уметь:</b></p>

		<p>разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задач защиты информации</p> <p><b>Владеть:</b></p> <p>методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации</p>
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	<p><b>Знать:</b></p> <p>типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации;</p> <p><b>Уметь:</b></p> <p>определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств;</p>

		<p>работать с современной элементной базой электронной аппаратуры.</p> <p>определять направления использования ЭВМ определенного класса для решения служебных задач</p> <p><b>Владеть:</b></p> <p>навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности;</p> <p>навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования;</p> <p>навыками формирования структуры СВТ и выбора режимов их функционирования</p>
ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	<p><b>Знать:</b></p> <p>назначение, виды и принципы построения организации и управления службы защиты информации</p> <p><b>Уметь:</b></p> <p>применять современные компьютерные технологии для решения профессиональных задач;</p> <p>ориентироваться в сети научных и образовательных порталов сети Интернет;</p> <p>обрабатывать результаты полученных измерений с помощью математических программных продуктов</p> <p><b>Владеть:</b></p> <p>навыками работы с пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информацией</p>
ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	<p><b>Знать:</b></p> <p>основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности</p>

		<p>информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии</p> <p><b>Уметь:</b>  осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации</p> <p><b>Владеть:</b>  навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации</p>
--	--	---

### **3. УКАЗАНИЕ МЕСТА ПРОИЗВОДСТВЕННОЙ ЭКСПЛУАТАЦИОННОЙ ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Производственная эксплуатационная практика представляет собой дисциплину вариативной части (Б2.В.02(П)) блока Б2 «Практика» подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность» по профилю подготовки «Организация и технология защиты информации».

Логическая и содержательная связь дисциплин, участвующих в формировании представленных в п.1 компетенций, содержится в ниже представленной таблице:

<b>Код компетенции</b>	<b>Предшествующие дисциплины</b>	<b>Данная дисциплина</b>	<b>Последующие дисциплины</b>
ОПК-4	Информатика Введение в специальность Инженерная и компьютерная графика Языки программирования Операционные системы Базы данных Теория информации Криптографические методы защиты информации Программно-аппаратные средства защиты информации Основы построения многоканальных инфокоммуникационных систем и сетей Сети и системы передачи информации Учебная практика по получению первичных профессиональных умений и навыков	Производственная эксплуатационная практика	Квантовые методы защиты и обработки информации Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ОПК-5	Основы управления информационной безопасности Организационное и правовое обеспечение информационной безопасности Документоведение Метрология, стандартизация и сертификация		Защита и обработка конфиденциальных документов Производственная эксплуатационная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ОПК-7	Основы информационной безопасности Теория информации Теоретические основы компьютерной безопасности Учебная практика по получению первичных		Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы

	профессиональных умений и навыков		
ПК-1	<p>Теоретические основы компьютерной безопасности</p> <p>Криптографические методы защиты информации</p> <p>Техническая защита информации</p> <p>Программно-аппаратные средства защиты информации</p> <p>Распространение электромагнитных волн и антенно-фидерные устройства</p> <p>Основы электромагнитной совместимости</p> <p>Основы построения многоканальных инфокоммуникационных систем и сетей</p> <p>Сети и системы передачи информации</p> <p>Аппаратные средства вычислительной техники</p>		<p>Криптографические протоколы</p> <p>Защита в операционных системах</p> <p>Криптографические протоколы для защиты банковской информации</p> <p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p>
ПК-2	<p>Языки программирования</p> <p>Операционные системы</p> <p>Базы данных</p> <p>Теоретические основы компьютерной безопасности</p> <p>Цифровая обработка сигналов</p> <p>Криптографические методы защиты информации</p> <p>Программно-аппаратные средства защиты информации</p> <p>Учебная практика по получению первичных профессиональных умений и навыков</p>		<p>Криптографические протоколы</p> <p>Защита в операционных системах</p> <p>Защита программ и данных</p> <p>Основы построения защищенных баз данных</p> <p>Криптографические протоколы для защиты банковской информации</p> <p>Надежность, эргономика и качество информационных систем</p> <p>Производственная преддипломная практика</p>

			<p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p>
ПК-3	<p>Операционные системы</p> <p>Базы данных</p> <p>Теоретические основы компьютерной безопасности</p> <p>Программно-аппаратные средства защиты информации</p>		<p>Информационная безопасность корпоративных сетей</p> <p>Защита персональных данных в организации</p> <p>Аудит информационной безопасности автоматизированных систем</p> <p>Защита информации в кредитно-финансовых организациях</p> <p>Управление информационной безопасностью</p> <p>Стандарты информационной безопасности</p> <p>Организация и управление службой защиты информации</p> <p>Информационная безопасность автоматизированных систем</p> <p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p>



ПК-4	<p>Основы управления информационной безопасности  Информационная безопасность корпоративных сетей  Документоведение  Учебная практика по получению первичных профессиональных умений и навыков</p>		<p>Защита и обработка конфиденциальных документов  Защита персональных данных в организации  Аудит информационной безопасности автоматизированных систем  Защита информации в кредитно-финансовых организациях  Управление информационной безопасностью  Стандарты информационной безопасности  Организация и управление службой защиты информации  Информационная безопасность автоматизированных систем  Производственная эксплуатационная практика  Производственная преддипломная практика  Подготовка к процедуре защиты выпускной квалификационной работы  Процедура защиты выпускной квалификационной работы</p>
ПК-5	<p>Основы управления информационной безопасности  Организационное и правовое обеспечение информационной безопасности</p>		<p>Защита и обработка конфиденциальных документов  Управление информационной безопасностью</p>

	<p>Информационная безопасность корпоративных сетей Документоведение</p>		<p>Стандарты информационной безопасности Организация и управление службой защиты информации Информационная безопасность автоматизированных систем Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы</p>
ПК-6	<p>Основы управления информационной безопасности Организационное и правовое обеспечение информационной безопасности Техническая защита информации Программно-аппаратные средства защиты информации Аппаратные средства вычислительной техники</p>		<p>Управление информационной безопасностью Стандарты информационной безопасности Организация и управление службой защиты информации Информационная безопасность автоматизированных систем Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы</p>
ПК-7	<p>Организационное и правовое обеспечение информационной безопасности</p>		<p>Информационная безопасность корпоративных сетей Защита персональных</p>

		<p>данных в организации</p> <p>Аудит информационной безопасности автоматизированных систем</p> <p>Криптографические протоколы</p> <p>Защита информации в кредитно-финансовых организациях</p> <p>Защита программ и данных</p> <p>Основы построения защищенных баз данных</p> <p>Криптографические протоколы для защиты банковской информации</p> <p>Надежность, эргономика и качество информационных систем</p> <p>Производственная проектно-технологическая практика</p> <p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты выпускной квалификационной работы</p> <p>Процедура защиты выпускной квалификационной работы</p>
ПК-8	<p>Основы управления информационной безопасности</p> <p>Организационное и правовое обеспечение информационной безопасности</p>	<p>Производственная проектно-технологическая практика</p> <p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты</p>

	Метрология, стандартизация и сертификация Учебная практика по получению первичных профессиональных умений и навыков		выпускной квалификационной работы Процедура защиты выпускной квалификационной работы Астрономия и астрофизика Космология
ПК-9	Основы информационной безопасности Квантовые методы защиты и обработки информации Учебная практика по получению первичных профессиональных умений и навыков		Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-10	Организационное и правовое обеспечение информационной безопасности		Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-11	Техническая защита информации Аппаратные средства вычислительной техники		Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-12	Техническая защита информации Аппаратные средства вычислительной техники		Производственная преддипломная практика Подготовка к процедуре защиты выпускной

			квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-13	Техническая защита информации Аппаратные средства вычислительной техники		Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-14	Основы управления информационной безопасности Элективные курсы по физической культуре и спорту		Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-15	Основы управления информационной безопасности		Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы

#### **4. УКАЗАНИЕ ОБЪЕМА ПРАКТИКИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТИ В НЕДЕЛЯХ И АКАДЕМИЧЕСКИХ ЧАСАХ.**

Производственная эксплуатационная практика проводится в 6-м учебном семестре в течение 4 недель. Трудоемкость учебной практики - 6

зачетных единиц (ЗЕ) и 216 академических часов.

## 5. СОДЕРЖАНИЕ ПРАКТИКИ

№ п/п	Этапы практики	Виды работы	Трудоёмкость, час.
1	Подготовительный (ознакомительный) этап	Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации.	2
2	Подготовительный (ознакомительный) этап	Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка	2
3	Подготовительный (ознакомительный) этап	Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики.	4
4	Основной этап	Ознакомление с деятельностью предприятия. Определение методов и средств защиты информации, используемых на предприятии. Выполнение практических заданий. Сбор материалов для отчетной документации. данного предприятия.	192
5	Заключительный этап	Подготовка отчетной документации, получение характеристики о работе руководителя практики, представление отчетной документации, прохождение промежуточной аттестации по практике. Систематизация и анализ выполненных заданий.	16
<b>Итого 3 З.Е.</b>			<b>108</b>
<b>* ЗЕ -зачетная единица</b>			

## 6. УКАЗАНИЕ ФОРМ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Студент выполняет программу производственной эксплуатационной практики в соответствии с планом-графиком практики и индивидуальным заданием на практику, утверждаемым учебно-методическим советом института, ведет дневник практики, который защищает после окончания практики. В зависимости от специализации подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Для текущего контроля посещаемости производственной эксплуатационной практики используется стандартный журнал посещения занятий, который будет вести руководитель практики.

Отчет о результатах прохождения производственной эксплуатационной практики заслушивается на заседании учебно-методического совета института.

Дневник производственной эксплуатационной практики представлен в Приложении 1.

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

### 7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках производственной эксплуатационной практики

Контролируемые модули, разделы (темы) практики	Индекс контролируемой компетенции (или её части)	Содержание компетенции	Оценочные средства по этапам формирования компетенций	
			Текущий контроль по практике	промежуточный контроль по практике
Подготовительный (ознакомительный) этап Проведение установочной конференции в форме контактной работы,	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	

знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации.	ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
Подготовительный (ознакомительный) этап Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	
	ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
	ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Устный опрос	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос	
	ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	Устный опрос	



ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос	
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Устный опрос	
ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Устный опрос	
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос	
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос	
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос	
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Устный опрос	
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку	Устный опрос	

		погрешности и достоверности их результатов		
	ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Устный опрос	
	ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Устный опрос	
	ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Устный опрос	
	ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Устный опрос	
Подготовительный (ознакомительный) этап Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	
	ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности		
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		
	ПК-1	Способностью выполнять		

		работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач		
	ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты		
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		
	ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации		
	ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации		
	ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений		
	ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов		

	ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности		
	ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Устный опрос	
	ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Устный опрос	
	ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Устный опрос	
	ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Устный опрос	
	ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Устный опрос	
	ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Устный опрос	
Основной этап Ознакомление с деятельностью	ОПК-4	Способностью понимать значение информации в развитии современного	Устный опрос	

<p>предприятия.  Определение методов и средств защиты информации, используемых на предприятии.  Выполнение практических заданий.  Сбор материалов для отчетной документации.  данного предприятия.</p>		общества, применять информационные технологии для поиска и обработки информации		
	ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
	ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Устный опрос	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос	
	ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	Устный опрос	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос	
	ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Устный опрос	
	ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и	Устный опрос	

	эффективности применяемых программных, программно-аппаратных и технических средств защиты информации		
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Устный опрос	
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос	
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос	
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Устный опрос	
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Устный опрос	
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Устный опрос	
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Устный опрос	
ПК-14	Способностью организовывать работу малого коллектива	Устный опрос	

		исполнителей в профессиональной деятельности		
	ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Устный опрос	
Заключительный этап Подготовка отчетной документации, получение характеристики о работе руководителя практики, представление отчетной документации, прохождение промежуточной аттестации по практике. Систематизация и анализ выполненных заданий.	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	
	ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
				зачет

**Этапы формирования компетенций в процессе освоения образовательной программы в рамках производственной эксплуатационной практики**

Индекс контролируемой компетенции	№ Учебной недели № Темы раздела дисциплины/модуля						
	41	41	41	42	43	44	44
	1	2	3	4	4	4	5
	Этапы формирования компетенции						
ОПК-4	+	+	+	+	+	+	+
ОПК-5	+	+	+	+	+	+	+
ОПК-7	+	+	+	+	+	+	+
ПК-1		+	+	+	+	+	
ПК-2		+	+	+	+	+	
ПК-3		+	+	+	+	+	
ПК-4		+	+	+	+	+	
ПК-5		+	+	+	+	+	
ПК-6		+	+	+	+	+	
ПК-7		+	+	+	+	+	
ПК-8		+	+	+	+	+	
ПК-9		+	+	+	+	+	
ПК-10		+	+	+	+	+	
ПК-11		+	+	+	+	+	
ПК-12		+	+	+	+	+	
ПК-13		+	+	+	+	+	
ПК-14		+	+	+	+	+	
ПК-15		+					



**7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования**  
**Критерии определения сформированности компетенций на различных этапах их формирования**

Показатели	ниже порогового	пороговый	достаточный	повышенный
<b>Критерии</b>	<p>Компетенция не сформирована. Студент не способен определить основные понятия, воспроизвести основные факты, идеи теории информационной безопасности, не знает основные методы решения типовых задач. Не умеет работать со справочной литературой, не способен представить результаты своей работы. Не владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, не способен применять информационные технологии для решения типовых задач</p>	<p>Компетенция сформирована на «удовлетворительно». Студент дает определения основных понятий, воспроизводит основные факты, идеи, теории информационной безопасности, знает основные методы решения типовых задач. Умеет работать со справочной литературой, представлять результаты своей работы. Владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, способен применять информационные технологии для решения типовых задач</p>	<p>Компетенция сформирована на «хорошо». Студент понимает связи между различными понятиями теории, аргументирует выбор метода решения задачи и умеет их применять на практике. Применяет методы решения задач в незнакомых ситуациях, умеет корректно выражать и аргументированно обосновывать положения предметной области знания. Способен применять информационные технологии для решения прикладных задач, адаптировать типовые технологии к решению практико-ориентированных задач.</p>	<p>Компетенция сформирована «отлично». Студент устанавливает связи между основными концепциями в предметной области, теориями дисциплинами. Оценивает достоверность полученного решения задачи, методы решения задачи и выбирает оптимальный метод, разрабатывает модели реальных процессов и ситуаций. Способен передавать результат проведенных исследований в виде конкретных рекомендаций в терминах предметной области знания, интерпретировать знания предметной области.</p>

Поскольку практически всякая учебная дисциплина призвана формировать сразу несколько компетенций, критерии оценки целесообразно формировать в два этапа.

1-й этап: определение критериев оценки отдельно по каждой формируемой компетенции. Сущность 1-го этапа состоит в определении шкал оценивания для оценивания отдельно взятой компетенции на основе продемонстрированного обучаемым уровня самостоятельности в применении полученных в ходе изучения учебной дисциплины, знаний, умений и навыков.

## Шкала оценивания компетенций

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины</p>	<p>Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне</p>	<p>Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке</p>	<p>Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи</p>

2-й этап: определение критериев для оценки уровня обученности по учебной дисциплине на основе комплексного подхода к уровню сформированности всех компетенций, обязательных к формированию в процессе изучения предмета. Сущность 2-го этапа определения критерия оценки по учебной дисциплине заключена в определении подхода к оцениванию на основе ранее полученных данных о сформированности каждой компетенции, обязательной к выработке в процессе изучения предмета. В качестве основного критерия при оценке обучаемого при определении уровня освоения учебной дисциплины наличие сформированных у него компетенций по результатам освоения учебной дисциплины.

Положительная оценка по дисциплине, может выставляться и при не полной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.

## Шкала оценивания сформированности компетенции в рамках дисциплины

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Уровень освоения дисциплины, при котором у обучаемого не сформировано более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции</p>	<p>При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность до-формирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно»</p>	<p>Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо».</p>	<p>Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90% сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций</p>

### **7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в производственной эксплуатационной практики**

#### **7.3.1 Вопросы для текущего контроля.**

**Целью устного опроса** является закрепление, углубление и систематизация знаний студентов, полученных в процессе прохождения и при самостоятельной работе; проведение устного опроса позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

#### **Проверяемые компетенции:**

Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)

Способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)

Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)

Способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)

Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению

информационной безопасности объекта защиты (ПК-4)

Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)

Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)

Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)

Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8)

Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)

Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)

Способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)

Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)

Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)

Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)

1. Описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие.
2. Определить виды информации ограниченного доступа, обрабатываемые предприятием.
3. Ознакомиться с формами организации производственного процесса и его технологическим обеспечением.
4. Выявить угрозы безопасности предприятия.
5. Проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности.
6. Изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации.
7. Изучить методы и средства защиты информации, применяемые на предприятии.
8. Изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта.
9. Разработать модель угроз для конкретной информационной системы предприятия.
10. Изучить основные обязанности должностных лиц в области защиты информации.
11. Проанализировать методы контроля в области защиты информации, используемые в организации.



12. Разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия.
13. Предложить перечень мероприятий по улучшению системы защиты информации на предприятии.
14. Оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности.
15. Провести анализ безопасности программных продуктов, используемых на предприятии.
16. Изучить возможные методы прогнозирования появления уязвимостей в программном коде.
17. Произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД.
18. Изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации.
19. Спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения.
20. Спроектировать систему физической защиты информации.
21. Разработать политику информационной безопасности предприятия.
22. Проанализировать систему компьютерной безопасности предприятия.
23. Изучить систему контроля и управления доступом предприятия.
24. Ознакомиться с системой защиты персональных данных в организации.
25. Изучить виды правонарушений при совершении компьютерных преступлений.

### **7.3.2. Промежуточный контроль по практике**

Промежуточный контроль осуществляется в виде устного отчета о результатах прохождения производственной эксплуатационной практики.

К промежуточному контролю допускаются студенты

- правильно заполнившие дневник производственной эксплуатационной

практики;

- получившие положительный отзыв руководителя практики.

#### **7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций**

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций по производственной эксплуатационной практике проводится в форме текущей и промежуточной аттестации.

Контроль текущей успеваемости обучающихся - текущая аттестация - проводится в процессе прохождения практики с целью определения уровня усвоения обучающимися знаний; формирования у них умений и навыков; своевременного выявления преподавателем недостатков в подготовке студентов и принятия необходимых мер по ее корректировке; совершенствованию методики обучения; организации учебной работы и оказания обучающимся индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:

- на занятиях (опрос, допуск к работам, выполнение работ);
- по результатам проверки качества материалов, собранных учащимися в ходе практики.

Промежуточная аттестация по практике проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков по производственной эксплуатационной практике требованиям ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» в форме зачета.

Зачет проводится после завершения практики в объеме рабочей учебной программы. Форма проведения зачета определяется учебно-методическим советом института (путем собеседования по вопросам; письменная работа, тестирование и

др.). Оценка по результатам зачета - «зачтено», «незачтено».

«Зачтено» ставится, если задания на практику выполнено в полном объёме, получен положительный отзыв руководителя практики, студент предоставил все необходимые материалы, оформил дневник практики, показана совокупность осознанных знаний. Знание по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной практики с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи.

«Зачтено» также ставится, если задания на практику выполнено в полном объёме, получен положительный отзыв руководителя практики от организации-партнёра, студент предоставил все необходимые материалы, оформил дневник практики дал развернутые ответы на поставленные вопросы, показал умение выделить существенные и несущественные признаки, причинно-следственные связи, но допустил 2-3 неточности или незначительные ошибки. Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне.

«Незачтено» ставится в случае, когда задания на практику выполнено не в полном объёме, отзыв руководителя практики от организации-партнёра, отрицателен, или студент не предоставил всех необходимых материалов, не

оформил по установленной форме дневник практики, или не показал в ходе собеседования совокупность осознанных знаний; присутствуют фрагментарность, нелогичность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента, или ответ на вопрос полностью отсутствует, или отказ от ответа. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения практики.

Все виды текущего контроля осуществляются в ходе решения производственных и иных задач.

Каждая форма контроля по дисциплине включает в себя теоретические вопросы, позволяющие оценить уровень освоения студентами знаний и практические задания, выявляющие степень сформированности умений и навыков.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки (на каждом занятии).
2. Многоступенчатость: оценка (как преподавателем, так и студентами группы) и самооценка обучающегося, обсуждение результатов и комплекса мер по устранению недостатков.
3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.
4. Соблюдение последовательности проведения оценки: предусмотрено, что развитие компетенций идет по возрастанию их уровней сложности, а оценочные средства на каждом этапе учитывают это возрастание.

Краткая характеристика процедуры реализации текущего и промежуточного контроля по дисциплине для оценки компетенций обучающихся представлена в таблице:

№ п/п	Наименование оценочного средства	Краткая характеристика процедуры оценивания компетенций	Представление оценочного средства в фонде
1	Устный опрос	Устный опрос по основным терминам может проводиться в начале/конце практического занятия в течение 15-20 мин.	Вопросы по темам/разделам дисциплины

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

### **Основная литература**

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ [Т. А. Полякова [и др.] ; под ред.: Т. А. Поляковой, А. А. Стрельцова. - Москва: Юрайт, 2019. - 1 on-line, 325 с.: рис.. - (Бакалавр и магистр. Академический курс)
2. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/13931.html>

### **Дополнительная литература**

1. Мельников, В. П. Информационная безопасность [Электронный ресурс]: [учеб. пособие]/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 8-е изд., испр.. - Москва: Академия, 2013. - 1 эл. опт. диск (CD-ROM), 336 с.: рис., табл.). - - Библиогр.: с. 327-328 (37 назв.)
2. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие для вузов/ Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР; Москва: Инфра-М, 2017. - 202, [1] с.: ил. - (Высшее образование). - Библиогр.: с. 195-198. - ISBN 978-5-369-01603-9. - ISBN

- 978-5-16-012372-1: 485.89, 485.89, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
3. Сагдеев, К. М. Физические основы защиты информации: учеб. пособие для вузов/ К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. - 2-е изд., испр. и доп.. - Санкт-Петербург: Интермедия, 2017. - 408 с.: ил. - Библиография: с. 405-406 (22 названия). - ISBN 978-5-4383-0141-7: 780.00, 780.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  4. Рагозин, Ю. Н. Инженерно-техническая защита информации: учеб. пособие по физ. основам образования техн. каналов утечки информации по практикуму оценки их опасности/ Ю. Н. Рагозин. - Санкт-Петербург: Интермедия, 2018. - 165 с.: ил.. - Библиогр.: с. 164-165 (31 назв.). - ISBN 978-5-4383-0161-5: 680.00, 680.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г. А. Бузов. - Москва: Горячая линия-Телеком, 2014. - 585, [4] л. вкл. с.: ил.. - Библиогр.: с. 574-581 (126 назв.). - ISBN 978-5-9912-0424-8: 712.80, 712.80, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  6. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации/ В. Я. Ищейнов, М. В. Мещатунян. - 2-е изд., перераб. и доп.. - Москва: Форум; Москва: ИНФРА-М, 2014. - 255 с. - (Высшее образование - бакалавриат). - Библиогр.: с. 251-253. - ISBN 978-5-91134-856-4. - ISBN 978-5-16-009578-3: 349.69, 349.69, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
  7. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации/ Г. А. Бузов. - М.: Горячая линия-Телеком, 2013. - 239 с.: ил. - Библиогр.: с. 230-235. - ISBN 978-5-9912-0121-6: 303.60, 303.60, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)

8. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 608-609 (34 назв.). - ISBN 978-5-9912-0084-4: 699.60, 699.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(14), ч.з.N3(1)

### Перечень интернет-источников

1. «Национальная электронная библиотека» (<http://xn--90ax2c.xn--p1ai/>).
2. ЭБС Кантиана (<https://elib.kantiana.ru/>).
3. ЭБС IPR BOOKS (<https://www.iprbookshop.ru/78574.html>).
4. ЭБС Znanium (<https://znanium.com/catalog/document?id=333215>).

## 9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

1. Использование системы электронного образовательного контента БФУ им. И. Канта <http://lms-3.kantiana.ru/>.
2. Использование электронной образовательной среды БФУ им. И. Канта <https://teams.microsoft.com/>

## 10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

<p>Лаборатория технических средств защиты информации Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, третий этаж, ауд. 315</p>	<p>Нелинейный локатор "Лорнет" Анализ спектра "СК-4 Белан-32" Антенна логопериодическая "ЕЛВ-26" Аппаратно-программный лабораторный комплекс средств защиты информации Анализатор проводных линий "ОТКЛИК" Аппаратно-программный комплекс защиты информации от несанкционированного доступа</p>	<p>Типовое программное обеспечение: Microsoft Windows 7 pro, Microsoft Office standart 2010 – договор №1980/12 14.12.2012 ООО "ЭСЭМДЖИ", акт АА-118 от 21.12.2012 Антивирусное программное обеспечение Kaspersky Endpoint Security договор № 1311/19 от 01.03.2019 ООО "СофтЛайн Проекты" акт Pr001333 от</p>
--	---	---

	<p>Программно-аппаратный комплекс "Навигатор-ПЗГ" АПКШ "Континент"</p> <p>Комплект специальных средств защиты информации от утечки по техническим каналам</p> <p>Программно-аппаратный комплекс автоматического обнаружения, идентификации и нейтрализации подслушивающих устройств "Крона"</p> <p>Комплекс многофункциональных поисковых приборов локализации каналов утечки информации</p> <p>Проектор Toshiba TDP-EX1 переносной</p> <p>Электронные наборы/модули СС1020ЕМК-433 Т1</p> <p>Инструментарий для модулей фирмы TI/СС СС1070ЕМ-433 Т1</p> <p>Инструментарий для модулей фирмы TI/СС СС1070ЕМ-433 Т1</p> <p>Инструментарий для модулей фирмы TI/СС СС1070ЕМ-433 Т1</p> <p>Инструментарий для модулей фирмы TI/СС СС1070ЕМ-433 Т1</p> <p>Паяльная станция-фен нагретым воздухом</p> <p>Осциллограф генератор PCSGU 250 usb</p> <p>Комплект оборудования для экспериментального стенда микропроцессорной техники</p> <p>Телевизор LG 42LW650S</p> <p>Персональный компьютер с параметрами - Intel Core I3-3220, 3.3 GHz, 4Gb RAM, 1 Tb HDD, 21,5", keyboard, Mouse, LAN, Internet access</p>	25.07.2019
<p>Учебная лаборатория для самостоятельной работы, для работы над курсовыми и дипломными проектами</p> <p>Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, четвертый этаж, ауд. 417</p>	<p>Телевизор LG 50LN540V</p> <p>Рабочие станции DEPO Race G540S (7 шт.);</p> <p>Мониторы 27" ViewSonic VX2739WM (7 шт.);</p> <p>Цветной лазерный принтер формата А3 Hewlett-Packard Color LaserJet Enterprise CP5525dn;</p> <p>Источники бесперебойного питания Mustek PowerMust 1590 (7 шт.);</p>	<p>Общесистемное программное обеспечение Microsoft Windows 7,</p> <p>Общесистемное программное обеспечение Microsoft Office Standart 2010 – Договор поставки № 952 от 19.10.2011 ООО «Джи-Кей Системс»</p>



	Цветной плоттер формата A1 Hewlett-Packard HP Designjet T790;	
--	---	--



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
**ФГАОУ ВО «БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА»**  
ИНСТИТУТ ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК И  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**ДНЕВНИК**  
**ПРОИЗВОДСТВЕННОЙ ЭКСПЛУАТАЦИОННОЙ ПРАКТИКИ**

*Студента 3 курса*

*Направления подготовки 10.03.01 «Информационная безопасность»*

*Профиль подготовки «Организация и технология защиты информации»*

*Иванова Ивана Ивановича*

Калининград

20\_\_ год

1. Фамилия *Иванов*
2. Имя и отчество *Иван Иванович*
3. Курс 3
4. Направление подготовки 10.03.01 «Информационная безопасность»,  
Профиль подготовки «Организация и технология защиты информации»
5. Место прохождения практики \_\_\_\_\_  
\_\_\_\_\_
6. Срок практики \_\_.\_\_.\_\_\_\_-\_\_.\_\_.\_\_\_\_
7. Руководитель практики от института физико-математических наук и информационных технологий \_\_\_\_\_ / \_\_\_\_\_  
«\_\_» \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП \_\_\_\_\_ Бурмистров В. И.

печать

### *Даты прохождения практики*

Прибыл на место практики «\_\_» \_\_\_\_\_ 20\_\_ г

Назначен \_\_\_\_\_ практикантом  
Рабочее место, должность

Откомандирован в БФУ им. И. Канта «\_\_» \_\_\_\_\_ 20\_\_ г

Первый заместитель директора ИФМНиИТ

\_\_\_\_\_ Шпилевой А. А.  
подпись и печать

## ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

«УТВЕРЖДАЮ»

Руководитель практики от БФУ им. И. Канта

\_\_\_\_\_ / \_\_\_\_\_ /  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

для \_\_\_\_\_,  
(ФИО студента)

Место прохождения: \_\_\_\_\_

Срок прохождения: с «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_.

Цель прохождения: \_\_\_\_\_

Задачи: \_\_\_\_\_

### Содержание:

1	Подготовительный этап	Ознакомление с программой практики
		Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации
2	Основной этап	Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка
		...
		...
3	Заключительный этап	Сбор материалов для дневника практики.
		Оформление дневника практики в электронном и печатном виде

### Планируемые результаты:

1	
2	
3	
4	
5	
...	

Форма отчетности: \_\_\_\_\_

Форма контроля: \_\_\_\_\_

Ознакомлен(а) \_\_\_\_\_  
(подпись студента)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.



	Выходной					
__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__	__.__.20__
	Выходной				Сбор материалов для дневника практики.	Оформление дневника практики в электронном и печатном виде.

***Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.***

Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка проведен \_\_.\_\_.20\_\_ г.

С требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка ознакомлен \_\_.\_\_.20\_\_ г.

\_\_\_\_\_ / \_\_\_\_\_

Подпись ответственного за проведение инструктажей

\_\_\_\_\_ / \_\_\_\_\_  
подпись и печать

## *Повседневный план производственной эксплуатационной практики*

<i>Дата</i>	<i>Выполненные работы</i>	<i>Подпись руководителя практики</i>
__ . __ . 20 __	Ознакомление с программой практики. Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации. Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.	
__ . __ . 20 __		Выходной
__ . __ . 20 __	<i>Подробное описание видов работ</i>	
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __	Сбор материалов для дневника практики.	
__ . __ . 20 __	Оформление дневника практики в электронном и печатном виде.	



**Список материалов,  
собранных студентом в период прохождения практики**

№ п/п	
1.	
2.	
3.	
4.	
5.	
6.	

**Характеристика работы студента руководителем практики**  
(указанием степени его теоретической подготовки, качества выполненной работы, трудовой дисциплины и недостатков, если они имели место)

Ruled area for writing the characteristic of the student's work.

Подпись руководителя практики \_\_\_\_\_

«\_» \_\_\_\_\_ 20\_\_ г.



## **ПРИЛОЖЕНИЕ**

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА**

**Институт физико-математических наук и информационных технологий**

«Согласовано»

Ведущий менеджер ООП ИФМНиИТ  
В.И.Бурмистров

«10» марта 2020 г.

«Утверждено»

Директор ИФМНиИТ  
А.В.Юров

«10» марта 2020 г.



**ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ ПО ПОЛУЧЕНИЮ ПЕРВИЧНЫХ  
ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И НАВЫКОВ**

для студентов 2 курса  
очной формы обучения

направления подготовки 10.03.01.

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

профиль подготовки **«ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ  
ИНФОРМАЦИИ»**

уровень высшего образования – бакалавриат

Калининград, 2020 г.

## Лист согласования

**Составители:** доцент ИФМНиИТ, кандидат технических наук, доцент Ветров И. А.

Программа обсуждена и утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий.

Протокол № \_\_\_/\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Председатель учебно-методического совета \_\_\_\_\_ первый  
заместитель директора института, к.ф.-м.н., доцент, Шпилевой А. А.

Программа пересмотрена на заседании учебно-методического совета института физико-математических наук и информационных технологий. Внесены следующие изменения (или изменений не внесено) \_\_\_\_\_

Протокол № \_\_\_\_\_ от « \_\_\_ » \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП

\_\_\_\_\_ Бурмистров В. И.

## СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1. Указание вида практики, способа и формы ее проведения.....	4
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.....	4
3. Указание места практики в структуре образовательной программы.....	6
4. Указание объема практики в зачетных единицах и ее продолжительности в неделях и академических часах.....	8
5. Содержание практики.....	8
6. Указание форм отчетности по практике.....	8
7. Фонд оценочных средств проведения промежуточной аттестации обучающихся по практике.....	9
7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебно-лабораторной практики.....	9
7.2 Показатели и критерии оценивания компетенций на различных этапах их формирования.....	14
7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в рамках учебно-лабораторной практики.....	19
7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.....	21
8. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики.....	24
9. Перечень информационных технологий, используемых при проведении практики.....	25
10. Описание материально-технической базы, необходимой для проведения практики.....	26
Приложение 1.....	28

## **1. УКАЗАНИЕ ВИДА ПРАКТИКИ, СПОСОБА И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ**

**Вид практики:** учебная практика.

**Способ проведения** учебной практики: стационарная.

Стационарная практика проводится в образовательной организации, в которой обучающиеся осваивают образовательную программу, или в иных организациях, с которыми действуют соответствующие договорные отношения.

**Формы проведения** учебной практики: невыездная, непрерывная. Организация проведения производственной практики осуществляется путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения практики.

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

**Целями** учебной практики по получению первичных профессиональных умений и навыков являются:

- закрепление и расширение теоретических и практических знаний, полученных за время обучения;
- изучение литературы и нормативно-методической документации по профилю подготовки;
- ознакомление с содержанием основных работ и исследований, выполняемых в области информационной безопасности;
- приобретение заданных компетенций для будущей профессиональной деятельности;
- приобретение первоначальных практических навыков выполнения работ по обслуживанию технических средств защиты информации.

К основным **задачам** учебной практики по получению первичных



профессиональных умений и навыков относятся: ознакомление студента с сущностью и социальной значимостью своей будущей профессии, объектами и видами профессиональной деятельности, приобретение профессиональных компетенций и творческое развитие профессии и человека в ней, умение на научной основе организовать свой труд и владение компьютерными методами сбора, хранения и обработки (редактирования) информации, применяемыми в профессиональной деятельности, изучение техники безопасности, санитарно-гигиенических условий труда и противопожарных мероприятий при работе с использованием современных информационных технологий.

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Результаты освоения ООП	Перечень планируемых результатов обучения по дисциплине
ОК-5	Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	<p><b>Знать:</b>  об объектах информационной безопасности;  о направлениях защиты информации;  о требованиях к системам защиты информации</p> <p><b>Уметь:</b>  использовать основные принципы организации режима защиты информации  ориентироваться в вопросах, связанных с технологией защиты информации</p> <p><b>Владеть:</b>  навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования</p>
ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	<p><b>Знать:</b>  основные понятия и теоремы теории информации и кодирования;  основные принципы и способы кодирования и декодирования;  характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования;  методы исследования кодов и их применений в ЭВМ и системах защиты информации</p> <p><b>Уметь:</b>  вычислять количество информации в сообщениях дискретного источника канала связи;  кодировать и декодировать сообщения</p>

		<p>источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость;</p> <p><b>Владеть:</b>          средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом уровне</p>
ОПК-7	<p>Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	<p><b>Знать:</b>          способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности;</p> <p><b>Уметь:</b>          классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения;</p> <p><b>Владеть:</b>          навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания</p>

		<p>информационных процессов и особенностей функционирования объекта защиты; методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем;</p>
ПК-2	<p>Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>	<p><b>Знать:</b> задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; способы и механизмы администрирования подсистем информационной безопасности, критерии эффективности применения СЗИ.</p> <p><b>Уметь:</b> определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы.</p> <p><b>Владеть:</b></p>

		<p>способами, механизмами администрирования средств защиты информации и средств, встроенных в ОС;</p> <p>программным обеспечением сканирования уязвимостей и аудита эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p>
ПК-4	<p>Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p><b>Знать:</b></p> <p>структуру системы управления информационной безопасностью;</p> <p>приемы управлению информационной безопасностью</p> <p>методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз</p> <p><b>Уметь:</b></p> <p>выделять процессы управления информационной безопасностью защищаемых объектов,</p> <p>разрабатывать предложения по совершенствованию системы управления информационной безопасностью;</p> <p>выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации;</p> <p>обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте.</p> <p><b>Владеть:</b></p> <p>правилами, процедурами, практические приемы и пр. для управления информационной безопасности</p> <p>системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты</p> <p>методами и средствами минимизации угроз за счет совершенствования процессов управления</p>
ПК-8	<p>Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p>	<p><b>Знать:</b></p> <p>правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;</p> <p>правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;</p> <p>основные отечественные и зарубежные стандарты в области компьютерной безопасности;</p>

		<p>терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности в компьютерной сфере; направления создания правовой базы в области информационной безопасности; области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну</p> <p><b>Уметь:</b>  применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;</p> <p><b>Владеть:</b>  навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках; навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической</p>
--	--	---

		документацией на компоненты компьютерных систем на русском и иностранном языках; навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; разработке специализированной проектной и технической документации
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	<p><b>Знать:</b>  место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России  законодательство Российской Федерации, государственные стандарты и нормативные документы по защите информации, основные общеметодологические принципы теории информационной безопасности  стандарты и нормативные документы по защите информации, в том числе международные</p> <p><b>Уметь:</b>  классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности  систематизировать информацию, формулировать требования к защищаемым системам на основе требований нормативных и правовых документов</p> <p><b>Владеть:</b>  профессиональной терминологией в области информационной безопасности  средствами поиска, методами обобщения нормативных и методических материалов в сфере своей профессиональной деятельности, средствами поиска, обобщения научно-технической информации, нормативных и методических материалов, отечественного и зарубежного опыта в сфере своей профессиональной деятельности</p>

### 3. УКАЗАНИЕ МЕСТА УЧЕБНО-ЛАБОРАТОРНОЙ ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная практика по получению первичных профессиональных умений и навыков представляет собой дисциплину вариативной части (Б2.В.01(У)) блока Б2 «Практика» подготовки студентов по направлению подготовки 10.03.01

«Информационная безопасность» по профилю подготовки «Организация и технология защиты информации».

Логическая и содержательная связь дисциплин, участвующих в формировании представленных в п.1 компетенций, содержится в ниже представленной таблице:

<b>Код компетенции</b>	<b>Предшествующие дисциплины</b>	<b>Данная дисциплина</b>	<b>Последующие дисциплины</b>
ОК-5	Введение в специальность Основы информационной безопасности	Учебная практика по получению первичных профессиональных умений и навыков	Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ОПК-4	Информатика Введение в специальность Инженерная и компьютерная графика Языки программирования Операционные системы Базы данных Теория информации		Криптографические методы защиты информации Программно-аппаратные средства защиты информации Квантовые методы защиты и обработки информации Основы построения многоканальных инфокоммуникационных систем и сетей Сети и системы передачи информации Производственная эксплуатационная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ОПК-7	Основы информационной безопасности Теория информации Теоретические основы компьютерной безопасности		Производственная эксплуатационная практика Подготовка к процедуре защиты выпускной квалификационной работы

			Процедура защиты выпускной квалификационной работы
ПК-2	Языки программирования Операционные системы Базы данных Теоретические основы компьютерной безопасности Цифровая обработка сигналов		Криптографические методы защиты информации Программно-аппаратные средства защиты информации Криптографические протоколы Защита в операционных системах Защита программ и данных Основы построения защищенных баз данных Криптографические протоколы для защиты банковской информации Надежность, эргономика и качество информационных систем Производственная эксплуатационная практика Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
ПК-4	Основы управления информационной безопасности		Информационная безопасность корпоративных сетей Документоведение Защита и обработка конфиденциальных документов Защита персональных данных в организации Аудит информационной безопасности автоматизированных систем Защита информации в



		<p>кредитно-финансовых организациях  Управление информационной безопасностью  Стандарты информационной безопасности  Организация и управление службой защиты информации  Информационная безопасность автоматизированных систем  Производственная эксплуатационная практика  Производственная преддипломная практика  Подготовка к процедуре защиты выпускной квалификационной работы  Процедура защиты выпускной квалификационной работы</p>
ПК-8	<p>Основы управления информационной безопасностью  Метрология, стандартизация и сертификация</p>	<p>Организационное и правовое обеспечение информационной безопасности  Производственная эксплуатационная практика  Производственная проектно-технологическая практика  Производственная преддипломная практика  Подготовка к процедуре защиты выпускной квалификационной работы  Процедура защиты выпускной квалификационной работы  Астрономия и астрофизика  Космология</p>

ПК-9	Основы информационной безопасности		Квантовые методы защиты и обработки информации Учебная практика по получению первичных профессиональных умений и навыков Производственная эксплуатационная практика Производственная преддипломная практика Подготовка к процедуре защиты выпускной квалификационной работы Процедура защиты выпускной квалификационной работы
------	------------------------------------	--	---

#### 4. УКАЗАНИЕ ОБЪЕМА ПРАКТИКИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТИ В НЕДЕЛЯХ И АКАДЕМИЧЕСКИХ ЧАСАХ.

Учебная практика по получению первичных профессиональных умений и навыков проводится в 4-м учебном семестре в течение 2 недель. Трудоемкость учебной практики - 3 зачетных единиц (ЗЕ) и 108 академических часов.

#### 5. СОДЕРЖАНИЕ ПРАКТИКИ

№ п/п	Этапы практики	Виды работы	Трудоёмкость, час.
1	Основной этап	Ознакомительная информация, собрание	2
2	Основной этап	Инструктаж по технике	2
3	Основной этап	Сбор фактического и литературного материала, выполнение	80
4	Основной этап	Обработка, систематизация фактического и	8
5	Подготовка отчётной документации по итогам практики	Подготовка дневника практики	16
<b>Итого 3 З.Е.</b>			<b>108</b>
* ЗЕ -зачетная единица			

## 6. УКАЗАНИЕ ФОРМ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Студент выполняет программу учебной практики в соответствии с планом-графиком практики и индивидуальным заданием на практику, утверждаемым учебно-методическим советом института, ведет дневник практики, который защищает после окончания практики. В зависимости от специализации подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Для текущего контроля посещаемости учебной практики используется стандартный журнал посещения занятий, который будет вести руководитель практики.

Отчет о результатах прохождения учебной практики заслушивается на заседании учебно-методического совета института.

Дневник учебной практики представлен в Приложении 1.

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

### 7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной практики

Контролируемые модули, разделы (темы) практики	Индекс контролируемой компетенции (или её части)	Содержание компетенции	Оценочные средства по этапам формирования компетенций	
			Текущий контроль по практике	промежуточный контроль по практике
Основной этап Ознакомительная информация, собрание	ОК-5	Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения	Устный опрос	

		информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		
	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
Основной этап Инструктаж по технике	ОК-5	Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Устный опрос	
	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания	Устный опрос	

		информационных процессов и особенностей функционирования объекта защиты		
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос	
	ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос	
	ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос	
Основной этап Сбор фактического и литературного материала, выполнение практических задач	ОК-5	Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Устный опрос	
	ОПК-4	Способностью понимать	Устный	

		значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос	
	ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос	
	ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос	
Основной этап Обработка,	ОК-5	Способностью понимать социальную значимость своей	Устный опрос	

систематизация фактического и литературного материала		будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		
	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
	ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Устный опрос	
	ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Устный опрос	
	ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Устный опрос	

	ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Устный опрос	
Подготовка отчётной документации по итогам практики Подготовка дневника практики	ОК-5	Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Устный опрос	
	ОПК-4	Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Устный опрос	
	ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос	
				зачет



**Этапы формирования компетенций в процессе освоения образовательной программы в рамках учебной практики**

Индекс контролируемой компетенции	№ Учебной недели № Темы раздела дисциплины/модуля					
	43	43	43	44	44	44
	1	2	3	3	4	5
	Этапы формирования компетенции					
ОК-5	+	+	+	+	+	+
ОПК-4	+	+	+	+	+	+
ОПК-7	+	+	+	+	+	+
ПК-2		+	+	+	+	
ПК-4		+	+	+	+	
ПК-8		+	+	+	+	
ПК-9		+	+	+	+	

**7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования**  
**Критерии определения сформированности компетенций на различных этапах их формирования**

Показатели	ниже порогового	пороговый	достаточный	повышенный
<b>Критерии</b>	Компетенция не сформирована. Студент не способен определить основные понятия, воспроизвести основные факты, идеи теории информационной безопасности, не знает основные методы решения типовых задач. Не умеет работать со справочной литературой, не способен представить результаты своей работы. Не владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, не способен применять информационные технологии для решения типовых задач	Компетенция сформирована на «удовлетворительно». Студент дает определения основных понятий, воспроизводит основные факты, идеи, теории информационной безопасности, знает основные методы решения типовых задач. Умеет работать со справочной литературой, представлять результаты своей работы. Владеет основной терминологией в предметной области, начальными навыками в области информационной безопасности, способен применять информационные технологии для решения типовых задач	Компетенция сформирована на «хорошо». Студент понимает связи между различными понятиями теории, аргументирует выбор метода решения задачи и умеет их применять на практике. Применяет методы решения задач в незнакомых ситуациях, умеет корректно выражать и аргументированно обосновывать положения предметной области знания. Способен применять информационные технологии для решения прикладных задач, адаптировать типовые технологии к решению практико-ориентированных задач.	Компетенция сформирована «отлично». Студент устанавливает связи между основными концепциями в предметной области, теориями дисциплинами. Оценивает достоверность полученного решения задачи, методы решения задачи и выбирает оптимальный метод, разрабатывает модели реальных процессов и ситуаций. Способен передавать результат проведенных исследований в виде конкретных рекомендаций в терминах предметной области знания, интерпретировать знания предметной области.

Поскольку практически всякая учебная дисциплина призвана формировать сразу несколько компетенций, критерии оценки целесообразно формировать в два этапа.

1-й этап: определение критериев оценки отдельно по каждой формируемой компетенции. Сущность 1-го этапа состоит в определении шкал оценивания для оценивания отдельно взятой компетенции на основе продемонстрированного обучаемым уровня самостоятельности в применении полученных в ходе изучения учебной дисциплины, знаний, умений и навыков.

## Шкала оценивания компетенций

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины</p>	<p>Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне</p>	<p>Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке</p>	<p>Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи</p>

2-й этап: определение критериев для оценки уровня обученности по учебной дисциплине на основе комплексного подхода к уровню сформированности всех компетенций, обязательных к формированию в процессе изучения предмета. Сущность 2-го этапа определения критерия оценки по учебной дисциплине заключена в определении подхода к оцениванию на основе ранее полученных данных о сформированности каждой компетенции, обязательной к выработке в процессе изучения предмета. В качестве основного критерия при оценке обучаемого при определении уровня освоения учебной дисциплины наличие сформированных у него компетенций по результатам освоения учебной дисциплины.

Положительная оценка по дисциплине, может выставляться и при не полной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.

## Шкала оценивания сформированности компетенции в рамках дисциплины

Оценка «неудовлетворительно» или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
<p>Уровень освоения дисциплины, при котором у обучаемого не сформировано более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции</p>	<p>При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность до-формирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно»</p>	<p>Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо».</p>	<p>Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90% сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций</p>

### **7.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в рамках учебной практики**

#### **7.3.1 Вопросы для текущего контроля.**

**Целью устного опроса** является закрепление, углубление и систематизация знаний студентов, полученных в процессе прохождения и при самостоятельной работе; проведение устного опроса позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

#### **Проверяемые компетенции:**

Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5)

Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)

Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)

Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)

Способностью оформлять рабочую техническую документацию с учетом

действующих нормативных и методических документов (ПК-8)

Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

1. Информационная безопасность в системе национальной безопасности РФ.
2. Влияние процессов информатизации общества на составляющие информационной безопасности.
3. Состав и содержание направлений информационной безопасности.
4. Анализ угроз информационной безопасности.
5. Информационное противоборство.
6. Виды информации с точки зрения информационной безопасности.
7. Информационная безопасность. Методы и средства защиты информации.
8. Проблемы региональной безопасности.
9. Государственная информационная политика. История, становление, сущность и содержание, основные направления.
10. Причины, виды, каналы утечки и искажение информации.
11. Особенности подготовки по направлению подготовки 10.03.01 в соответствии со ФГОС ВО.
12. Отечественные и зарубежные стандарты в области информационной безопасности.
13. Информационная безопасность социальных взаимодействий.
14. Информационная безопасность информационно-управляющих систем.
15. Защита информации в системе дистанционного банковского обслуживания.
16. Правовые основы защиты персональных данных.
17. Криптография и основные этапы ее становления и развития.
18. Комплексный подход к обеспечению информационной безопасности.
19. Основные направления защиты информации.



20. Правовое обеспечение информационной безопасности.
21. Инженерно-техническое обеспечение информационной безопасности.
22. Организационное обеспечение информационной безопасности.
23. Информационное оружие. Виды и основы применения.
24. Организация работы с персоналом в системе информационной безопасности.
25. Основные нормативно-правовые акты в области информационной безопасности.
26. Основные направления обеспечения компьютерной безопасности.
27. Исторические этапы развития системы защиты информации в России.
28. Экономические факторы обеспечения безопасности коммерческой организации.
29. Политика информационной безопасности предприятия и организации.
30. Обучение персонала в системе обеспечения информационной безопасности.

### **7.3.2. Промежуточный контроль по практике**

Промежуточный контроль осуществляется в виде устного отчета о результатах прохождения учебно-лабораторной практики.

К промежуточному контролю допускаются студенты

- правильно заполнившие дневник учебно-лабораторной практики;
- получившие положительный отзыв руководителя практики.

### **7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций**

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций по учебной практике проводится в форме текущей и промежуточной аттестации.

Контроль текущей успеваемости обучающихся - текущая аттестация -

проводится в процессе прохождения практики с целью определения уровня усвоения обучающимися знаний; формирования у них умений и навыков; своевременного выявления преподавателем недостатков в подготовке студентов и принятия необходимых мер по ее корректировке; совершенствованию методики обучения; организации учебной работы и оказания обучающимся индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:

- на занятиях (опрос);
- по результатам проверки качества материалов, собранных учащимися в ходе практики.

Промежуточная аттестация по практике проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков по учебной практике требованиям ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» в форме зачета.

Зачет проводится после завершения практики в объеме рабочей учебной программы. Форма проведения зачета определяется учебно-методическим советом института (путем собеседования по вопросам; письменная работа, тестирование и др.). Оценка по результатам зачета - «зачтено», «незачтено».

«Зачтено» ставится, если задания на практику выполнено в полном объёме, получен положительный отзыв руководителя практики, студент предоставил все необходимые материалы, оформил дневник практики, показана совокупность осознанных знаний. Знание по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной практики с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной

компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи.

«Зачтено» также ставится, если задания на практику выполнено в полном объеме, получен положительный отзыв руководителя практики от организации-партнёра, студент предоставил все необходимые материалы, оформил дневник практики дал развернутые ответы на поставленные вопросы, показал умение выделить существенные и несущественные признаки, причинно-следственные связи, но допустил 2-3 неточности или незначительные ошибки. Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне.

«Незачтено» ставится в случае, когда задания на практику выполнено не в полном объеме, отзыв руководителя практики от организации-партнёра, отрицателен, или студент не предоставил всех необходимых материалов, не оформил по установленной форме дневник практики, или не показал в ходе собеседования совокупность осознанных знаний; присутствуют фрагментарность, нелогичность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента, или ответ на вопрос полностью отсутствует, или отказ от ответа. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения практики.

Все виды текущего контроля осуществляются в ходе решения производственных и иных задач.

Каждая форма контроля по дисциплине включает в себя теоретические вопросы, позволяющие оценить уровень освоения студентами знаний и практические задания, выявляющие степень сформированности умений и навыков.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки (на каждом занятии).
2. Многоступенчатость: оценка (как преподавателем, так и студентами группы) и самооценка обучающегося, обсуждение результатов и комплекса мер по устранению недостатков.
3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.
4. Соблюдение последовательности проведения оценки: предусмотрено, что развитие компетенций идет по возрастанию их уровней сложности, а оценочные средства на каждом этапе учитывают это возрастание.

Краткая характеристика процедуры реализации текущего и промежуточного контроля по дисциплине для оценки компетенций обучающихся представлена в таблице:

№ п/п	Наименование оценочного средства	Краткая характеристика процедуры оценивания компетенций	Представление оценочного средства в фонде
1	Устный опрос	Устный опрос по основным терминам может проводиться в начале/конце практического занятия в течение 15-20 мин.	Вопросы по темам/разделам дисциплины

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

### **Основная литература**

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/bcode/434171>

## Дополнительная литература

1. Галатенко, В. А. Основы информационной безопасности: курс лекций : учеб. пособие для студентов вузов/ В. А. Галатенко ; ред. В. Б. Бетелин; Интернет-Ун-т Информ. технологий. - 2-е изд., испр.. - М.: ИНТУИТ.РУ, 2004. - 260 с. - (Основы информационных технологий). - Библиогр.: с. 255-260. - ISBN 5-9556-0015-9: 159.20 р. Имеются экземпляры в отделах /There are copies in departments: НА(1)
2. Основы информационной безопасности: учеб. пособие/ Е. Б. Белов [и др.]. - М.: Горячая линия-Телеком, 2006. - 544 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр. в конце частей. - ISBN 5-93517-292-5: 316.25, 351.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 16: УБ(14), ч.з.N3(1), НА(1)
3. Горбенко, А. О. Основы информационной безопасности (введение в профессию): учеб. пособие для вузов/ А. О. Горбенко. - Санкт-Петербург: Интермедия, 2016. - 336 с.. - Библиогр.: с. 331. - ISBN 978-5-4383-0136-3: 663.00, 663.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
4. Горбенко, А. О. Основы информационной безопасности (введение в профессию): учеб. пособие для вузов/ А. О. Горбенко. - Санкт-Петербург: Интермедия, 2017. - 336 с. - Библиогр.: с. 331-336. - ISBN 978-5-4383-0136-3: 680.00, 680.00, р. Имеются экземпляры в отделах /There are copies in departments: НА(1)

## Перечень интернет-источников

1. «Национальная электронная библиотека» (<http://xn--90ax2c.xn--p1ai/>).
2. ЭБС Кантиана (<https://elib.kantiana.ru/>).
3. ЭБС IPR BOOKS (<https://www.iprbookshop.ru/78574.html>).
4. ЭБС Znanium (<https://znanium.com/catalog/document?id=333215>).

## 9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

1. Использование системы электронного образовательного контента БФУ им. И. Канта <http://lms-3.kantiana.ru/>.
2. Использование электронной образовательной среды БФУ им. И. Канта <https://teams.microsoft.com/>

## 10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

<p>Учебная аудитория для проведения занятий семинарского типа (компьютерный класс), Учебная аудитория для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, первый этаж, ауд. 122</p>	<p>Моноблок MSI AE 222 G -15 шт., Моноблок MSI AE 228 1G -5 шт., Моноблок MSI AE 228 2G -5 шт. ЖК телевизор LG</p>	<p>Типовое программное обеспечение: Microsoft Windows 7 pro, Microsoft Office standart 2010 – договор №1980/12 14.12.2012 ООО "ЭСЭМДЖИ", акт АА-118 от 21.12.2012 Антивирусное программное обеспечение Kaspersky Endpoint Security договор № 1311/19 от 01.03.2019 ООО "СофтЛайн Проекты" акт Pt001333 от 25.07.2019 Autodesk AutoCAD согласно Autodesk Account университета administrator@kantiana.ru Delphi 7 Lite Full Edition 7.3.4.3 лицензия GNU GPL Java 8 лицензия GNU GPL Maple договор 494/07 от 09.11.2007 ЗАО "СофтЛайн Трейд" Mathcad договор 494/07 от 09.11.2007 ЗАО "СофтЛайн Трейд" MATLAB договор 494/07 от 09.11.2007 ЗАО "СофтЛайн Трейд" Microsoft SQL Server договор № 494/12 от 4.04.12 ЗАО "СофтЛайн Трейд" Microsoft Visual Studio Professional № 494/12 от 4.04.12 ЗАО "СофтЛайн Трейд" Python 3.7.0 (Anaconda3 5.3.1 64-bit) лицензия BSD и Python Software Foundation License КОМПАС-3D V15.2 x64, КОМПАС-3D: Машиностроительная</p>
---	--	--

		конфигурация V15.2 x64, КОМПАС-3D: Приборостроительная конфигурация V15.2 x64, КОМПАС-3D: Строительная конфигурация V15.2 x64 договор 1201/15 от 02.06.15 ООО "АСКОН- Северо-Запад"
Учебная аудитория для проведения занятий семинарского типа (компьютерный класс), Учебная аудитория для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, третий этаж, ауд. 324	Рабочая станция Fujitsu Celsius W530 Power -12 шт; монитор DELL U2412M -12 шт; ИБП Back UPS APC 1100 -12 шт; Проектор Promethean DLP; интерактивная доска Promethean Active Board; Телевизор LG 50LB561V, LG 55LB561V	Общесистемное программное обеспечение Microsoft Windows 7, Общесистемное программное обеспечение Microsoft Office Standart 2013 - Договор поставки № 1698 от 30.10.2014 ООО «Балтийский поставщик»
Учебная лаборатория для самостоятельной работы, для работы над курсовыми и дипломными проектами Россия, 236016, Калининградская обл., г. Калининград, ул. А. Невского, дом № 14, корпус №2, четвертый этаж, ауд. 417	Телевизор LG 50LN540V Рабочие станции DEPO Race G540S (7 шт.); Мониторы 27" ViewSonic VX2739WM (7 шт.); Цветной лазерный принтер формата А3 Hewlett-Packard Color LaserJet Enterprise CP5525dn; Источники бесперебойного питания Mustek PowerMust 1590 (7 шт.); Цветной плоттер формата А1 Hewlett-Packard HP Designjet T790;	Общесистемное программное обеспечение Microsoft Windows 7, Общесистемное программное обеспечение Microsoft Office Standart 2010 – Договор поставки № 952 от 19.10.2011 ООО «Джи-Кей Системс»



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ФГАОУ ВО «БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ  
ИММАНУИЛА КАНТА»  
ИНСТИТУТ ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК И  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**ДНЕВНИК**  
**УЧЕБНОЙ ПРАКТИКИ ПО ПОЛУЧЕНИЮ ПЕРВИЧНЫХ**  
**ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И НАВЫКОВ**

*Студента 2 курса*

*Направления подготовки 10.03.01 «Информационная безопасность»*

*Профиль подготовки «Организация и технология защиты информации»*

*Иванова Ивана Ивановича*

Калининград

20\_\_ год



1. Фамилия **Иванов**
2. Имя и отчество **Иван Иванович**
3. Курс 2
4. Направление подготовки 10.03.01 «Информационная безопасность»,  
Профиль подготовки «Организация и технология защиты информации»
5. Место прохождения практики \_\_\_\_\_  
\_\_\_\_\_
6. Срок практики \_\_.\_\_\_\_\_.20\_\_ - \_\_.\_\_\_\_\_.20\_\_
7. Руководитель практики от института физико-математических наук и информационных технологий \_\_\_\_\_ / \_\_\_\_\_  
«\_\_» \_\_\_\_\_ 20\_\_ г.

Ведущий менеджер ООП \_\_\_\_\_ Бурмистров В. И.

печать

### *Даты прохождения практики*

Прибыл на место практики «\_\_» \_\_\_\_\_ 20\_\_ г

Назначен \_\_\_\_\_ практикантом  
Рабочее место, должность

Откомандирован в БФУ им. И. Канта «\_\_» \_\_\_\_\_ 20\_\_ г

Первый заместитель директора ИФМНиИТ

\_\_\_\_\_ Шпилевой А. А.  
подпись и печать

## ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

«УТВЕРЖДАЮ»

Руководитель практики от БФУ им. И. Канта

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

для \_\_\_\_\_,  
(ФИО студента)

Место прохождения: \_\_\_\_\_

Срок прохождения: с «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_

Цель прохождения: \_\_\_\_\_

Задачи: \_\_\_\_\_

### Содержание:

1	Подготовительный этап	Ознакомление с программой практики
		Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации
2	Основной этап	Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка
		...
		...
3	Заключительный этап	Сбор материалов для дневника практики.
		Оформление дневника практики в электронном и печатном виде

### Планируемые результаты:

1	
2	
3	
4	
5	
...	

Форма отчетности: \_\_\_\_\_

Форма контроля: \_\_\_\_\_

Ознакомлен(а) \_\_\_\_\_  
(подпись студента)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Календарный план-график учебной практики по получению первичных профессиональных умений и навыков**

___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__
<p>Ознакомление с программой практики.</p> <p>Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации.</p> <p>Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.</p>						Выходной
___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__	___. ___. 20__
				Сбор материалов для дневника практики.	Оформление дневника практики в электронном и печатном виде.	Выходной

***Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.***

Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка проведен \_\_.\_\_.20\_\_ г.

С требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка ознакомлен \_\_.\_\_.20\_\_ г.

\_\_\_\_\_ / \_\_\_\_\_

Подпись ответственного за проведение инструктажей

\_\_\_\_\_ / \_\_\_\_\_  
подпись и печать

***Повседневный план учебной практики по получению первичных профессиональных умений и навыков***

<i>Дата</i>	<i>Выполненные работы</i>	<i>Подпись руководителя практики</i>
__ . __ . 20 __	Ознакомление с программой практики. Ознакомление с формой отчётности по итогам практики и требованиями к оформлению документации. Инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка.	
__ . __ . 20 __	<i>Подробное описание видов работ</i>	
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		Выходной
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __		
__ . __ . 20 __	Сбор материалов для дневника практики.	
__ . __ . 20 __	Оформление дневника практики в электронном и печатном виде.	
__ . __ . 20 __		Выходной

**Список материалов,  
собранных студентом в период прохождения практики**

№ п/п	
1.	
2.	
3.	
4.	
5.	
6.	







## **ПРИЛОЖЕНИЕ**