Аннотации практик образовательной программы
по направлению 10.03.01 «Информационная безопасность»
Направленность/профиль *«Организация и технология защиты информации»*

Блок II.	Практики	Аннотации
	Практика по получению первичных профессиональных умений и навыков	Практика по получению первичных профессиональных умений и навыков является вариативной частью блока практик учебного плана. Реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой комплексной защиты информации. Цель практики: приобретение знаний и умений, необходимых для деятельности, связанной с эксплуатацией и обслуживанием современных средств вычислительной техники, а так же подготовка обучаемых к грамотному и эффективному использованию компьютера как инструмента для решения задач различной степени сложности в области компьютерной безопасности. Задачи: изучение основ вычислительной техники; изучение принципов работы ЭВМ; получение опыта самостоятельной диагностики, ремонта и настройки аппаратных средств вычислительной техники. Практика направлена на формирование следующих компетенций: • ОК-5 способность 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; • ПК-8 способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; • ПК-11 способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов. В результате освоения практики обучающийся должен: Знать: - социальную значимость своей будущей профессии. - основы делопроизводства, ведения технической документации с учетом действующих нормативных и методических документов. - структуру подсистем защиты информации и особенности работы с ними. Уметь: - понимать социальную значимость своей будущей профессии. - оформлять техническую документацию. - осуществлять выбор и настройку подсистем защиты информации, проводить оценку надёжности их функционирования. Владеть: - высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. - навыками ведения технической документации. - методами оценки эффективности работы подсистем защиты информации По практике предусмотрен текущий контроль в форме контроля посещаемости и составления отчёта, итоговая аттестация в форме зачета с оценкой. Общая трудоёмкость освоения дисциплины составляет 3 зачётных единицы.
	Эксплуатационная практика	Практика является вариативной частью блока практик учебного плана. Реализуется кафедрой информационной безопасности на базе организации, в соответствии с договором о практике. Цель эксплуатационной практики: закрепить знания и умения по организации и технологии защиты информации, приобретаемые студентами в процессе освоения теоретических курсов и специальных дисциплин. Выработать практические навыки и умения, способствующие комплексному формированию профессиональных

		компетенций студентов по овладению методами работы с конфиденциальными документами, усвоению организации закрытого делопроизводства в конкретных подразделениях объекта информатизации, приобретению профессиональных навыков и опыта работы в коллективе. Задачи практики: • закрепление знаний по разработке организационных мер по обеспечению информационной безопасности на конкретном объекте; • углубление теоретической подготовки и приобретение практических навыков и компетенций по проведению аналитических исследований по выявлению каналов распространения конфиденциальной информации; • овладение технологией проведения организационных мероприятий, направленных на предупреждение разглашения/утечки конфиденциальной информации; • овладение технологией работы с конфиденциальными документами, усвоению организации закрытого делопроизводства в конкретных подразделениях объекта информатизации; • приобретение практических навыков и компетенций по разработке нормативной и методической документации, регламентирующей организационную защиту информации, работе с конфиденциальными документами и построения защищенного документооборота на предприятии. Практика направлена на формирование общекультурных, а также профессиональных компетенций, соответствующих виду (видам) профессиональной деятельности - участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем: 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 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-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 ПК-14 - способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности В результате освоения практики обучающийся должен: Знать: - основные особенности Интернета как современной коммуникационной среды; - назначение и основные технические характеристики информационных систем, их взаимосвязь с техническими средствами охраны и видеонаблюдения;

		- основные руководящие, методические и нормативные документы по организационно-технической защите информации - основные принципы передачи информации; понятия инфраструктуры компьютерных сетей; требования к современным компьютерным сетям. - основные технические характеристики информационных систем; - основные руководящие, методические и нормативные документы по организационно-технической защите информации - основную научно-технической литературу, нормативные и методические документы в области обеспечения информационной безопасности - основные документы, выпускаемые регуляторами по информационной безопасности; - роль и место управления персоналом в организационном управлении и его связь со стратегическими задачами организации, работающей в области ИБ ; - причины многовариантности практики управления персоналом в современных условиях; - бизнес-процессы в сфере управления персоналом и роль в них линейных менеджеров и специалистов по управлению персоналом. - Порядок проведения контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок - Порядок проведения аттестации объектов вычислительной техники на соответствие требованиям по защите информации; - Порядок проведения аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации Уметь: - пользоваться основными сервисами Интернета; - описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз; - настраивать базовые настройки сетевых устройств 2го и 3го уровня; обнаруживать ошибки в настройке маршрутизации; пользоваться научно технической литературой в области компьютерных сетей. - оценивать возможную величину ущерба от реализации угроз; - описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз; - оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов - работать со стандартами и нормативными документами; - проводить аудит человеческих ресурсов организации, работающей в области ИБ, прогнозировать и определять потребность организации в персонале, определять эффективные пути ее удовлетворения; разрабатывать мероприятия по привлечению и отбору новых сотрудников и программы их адаптации; разрабатывать программы обучения сотрудников и оценивать их эффективность; использовать различные методы оценки и аттестации сотрудников и участвовать в их реализации; разрабатывать мероприятия по мотивированию и стимулированию персонала организации. - Провести контроль защищенности информации - установить, настроить, эксплуатировать и поддержать в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований Владеть: - правилами нетикета при работе в сети Интернет - методикой по разработке законодательных, организационно-режимных и технических решений по обеспечению безопасности объекта защиты - профессиональной терминологией; навыками настройки и эксплуатации коммуникационного оборудования

		- методикой по разработке технических решений по обеспечению безопасности объекта защиты - методикой по разработке законодательных, нормативных документов, технических решений по обеспечению безопасности объекта защиты - навыками использовать основы правовых знаний в различных сферах деятельности - навыками использования международных и национальных стандартов в своей профессиональной деятельности навыками организации работы малого коллектива исполнителей; навыками исследования системы управления персоналом; навыками анализа качественных и количественных данных; навыками выявления ключевых проблем в области управления персоналом. - методикой по разработке технических решений по обеспечению безопасности объекта защиты - администрированием подсистем информационной безопасности объекта; проведением аудита информационной безопасности автоматизированных систем По практике предусмотрен текущий контроль в форме контроля посещаемости и составления отчёта, итоговая промежуточная аттестация в форме зачёта с оценкой. Общая трудоемкость практики составляет 3 зачетных единиц.
	Проектно-технологическая практика	Практика является вариативной частью блока практик учебного плана. Реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Цель практики – углубление и закрепление теоретических знаний и практических навыков в области подготовки к аттестационным испытания автоматизированной системы и проведению таких испытаний по требованиям безопасности информации. Задачи практики: - изучение автоматизированной системы и технологического процесса обработки информации в ней; - формирование разрешительной системы доступа автоматизированной системы и реализация правил разграничения доступа средствами защиты информации; - проведение тестирования средств защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа; - исследование уязвимостей и угроз информационной безопасности в автоматизированной системе с последующей оценкой рисков. Практика направлена на формирование следующих компетенций: • ОК-5 - способность 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 • ПК-4 - способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты • ПК-5 - способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации • ПК-6 - способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации • ПК-7 - способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений • ПК-8- способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических

		документов • ПК-9 - способность 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 - способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности • ПК-11 - способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов • ПК-12 - способность принимать участие в проведении экспериментальных исследований системы защиты информации • ПК-13 - способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации • ПК-14- способностью организовывать работу малого коллектива 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 В результате освоения практики обучающийся должен: Знать технологический процесс обработки информации в автоматизированной системе; уязвимости и угрозы информационной безопасности. Уметь формировать разрешительную систему доступа автоматизированной системы; реализовывать правила разграничения доступа средствами защиты информации. Владеть навыками проведения тестирования средств защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа; навыками исследования уязвимостей и угроз информационной безопасности в автоматизированной системе. По практике предусмотрен текущий контроль в форме контроля посещаемости и составления отчёта, промежуточная аттестация в форме оценки отчета по практике – зачет с оценкой. Общая трудоёмкость освоения практики составляет 3 зачётные единицы.
	Преддипломная практика	Преддипломная практика (Пд) является вариативной частью блока практик учебного плана. Реализуется кафедрой информационной безопасности на базе организации, в соответствии с договором о практике. Цель преддипломной практики: Преддипломная практика направлена на расширение и углубление теоретических знаний, формирование умений и навыков выполнения разработки и проектирования в профессиональной сфере, подготовки технических отчетных документов, окончательную формулировку темы и содержания выпускной квалификационной работы (ВКР). Состоит в формировании заданных общекультурных, профессиональных и профессионально-специализированных компетенций, компетенций, обеспечивающих подготовку студентов к практической реализации эксплуатационных и экспериментально-исследовательских работ в области обеспечения информационной безопасности и защиты информации (ИБ и ЗИ). Задачи преддипломной практики: - выполнение этапов работы, определенных индивидуальным заданием, календарным планом, формой представления отчетных материалов и обеспечивающих выполнение планируемых в компетентностном

		формате результатов; - окончательное формулирование темы, содержания и перечня материалов, в том числе графических, выпускной квалификационной работы; - оформление отчета, содержащего материалы этапов и раскрывающего уровень освоения заданного перечня компетенций; - подготовка и проведение защиты полученных результатов. Практика направлена на формирование общекультурных, профессиональных и профессионально-специализированных компетенций по видам деятельности. 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 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-11 - способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов ПК-13 - способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ПК-14 - способностью организовывать работу малого коллектива 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 По профилю «Организация и технология защиты информации» ПСК-2.1 - способностью проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз информационной безопасности, вероятности их реализации и размера ущерба ПСК-2.2 - способностью формировать рекомендации по оптимизации функционального процесса объекта информатизации и разрабатывать комплекс организационно-технических мер по обеспечению информационной безопасности объекта защиты, с осуществлением его технико-экономического обоснования ПСК-2.3 - способностью организовать и принимать участие в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты, с разработкой необходимых для этого локальных нормативных документов ПСК-2.4 - способностью организовать контроль защищенности объекта информатизации в соответствии с нормативными документами В результате освоения практики обучающийся должен: Знать: - основные особенности Интернета как современной коммуникационной среды; - назначение и основные технические характеристики информационных систем, их взаимосвязь с техническими средствами охраны и видеонаблюдения; - основные руководящие, методические и нормативные документы по организационно-технической защите информации - терминологию процессов и систем защиты информации;

		- основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей; - основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах; - методологии и средства процессов и систем. - основные технические характеристики информационных систем; - основные направления политики предприятий в области обеспечения комплексной безопасности; особенности организационно-правового регулирования в области обеспечения комплексной безопасности. - закономерности развития предприятий различного типа и организацию их функционирования с целью достижения максимальной эффективности при минимальных затратах ресурсов; - виды и особенности рисков, порождаемых системами документооборота; - методы использования средств защиты информации при построении систем документооборота; - методы обеспечения юридической силы электронных данных; - основы действующего законодательства в области электронного документооборота - место и роль информационной безопасности в системе; - принципы построения системы управления информационной безопасностью в организации; - процессный подход к организации информационной безопасности; - нормативно-правовые и методологические основы информационной безопасности - Порядок проведения контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок - Порядок проведения аттестации объектов вычислительной техники на соответствие требованиям по защите информации; - Порядок проведения аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации Уметь: - пользоваться основными сервисами Интернета; - описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз; - использовать нормативно-правовые акты, регламентирующие вопросы определения угроз безопасности информации в информационных системах; - использовать принципы и методы процессов и систем защиты информации; - формулировать предложения по оптимизации и улучшению функционирования системы или процесса. - оценивать возможную величину ущерба от реализации угроз; - оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; - оценивать используемые системы документооборота с точки зрения обеспечения защищенности обрабатываемой информации и юридической силы электронных данных. - использовать нормативно-правовые акты по ИБ; - оценивать эффективность процессов управления ИБ организации; - оценивать эффективность СУИБ организации. - анализировать и оценивать текущее состояние ИБ на предприятии - исследовать полученные оценки информационной безопасности; - оценивать результаты и самооценки информационной безопасности.

		- Провести контроль защищенности информации - установить, настроить, эксплуатировать и поддержать в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований Владеть: - правилами нетикета при работе в сети Интернет - методикой по разработке законодательных, организационно-режимных и технических решений по обеспечению безопасности объекта защиты - терминологией в области процессов и систем защиты информации; - навыками использования правовых и нормативных требований к определению угроз безопасности информации в информационных системах; - формулирования предложений по оптимизации и улучшению функционирования системы или процесса. - методикой по разработке технических решений по обеспечению безопасности объекта защиты; - классификацией защищаемой информации по видам тайны; навыками подбора, изучения и обобщения научно-технической литературы, нормативных материалов по вопросам обеспечения информационной безопасности. - навыками использовать основы правовых знаний в различных сферах деятельности; - основной терминологией, методами и основными алгоритмами реализации процесса - терминологией и процессным подходом к построению СУИБ; - навыками анализа активов организации, угроз ИБ и уязвимостей в рамках области деятельности СУИБ; - методами научного исследования уязвимости и защищенности информационных процессов; - навыками использования методологии, правовых и нормативных требований и рекомендаций в области информационной безопасности. - методикой по разработке технических решений по обеспечению безопасности объекта защиты администрированием подсистем информационной безопасности объекта; проведением аудита информационной безопасности автоматизированных систем По практике предусмотрена предусмотрен текущий контроль в форме контроля посещаемости и составления отчёта, промежуточная аттестация в форме зачёта с оценкой. Общая трудоемкость практики составляет 9 зачетных единиц.