

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития
 Дата подписания: 05.06.2023 15:37:23

Аннотация дисциплины

Вид практики: b47f96ee5a16e179f04dbf7fb0b1000e3cd4d	Учебная	
Тип практики	Экспериментально-исследовательская практика	
Краткое содержание	Изучение основных правил организации научно-исследовательской и проектной работы в организации, а также управления коллективом; приобретение практических навыков в организации и проведении научных исследований, а также подготовки данных для составления обзоров, отчетов и научных публикаций; приобретение практических навыков в работе по обоснованию структуры и проектированию сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты; поведение анализа угроз информационной безопасности объектов и разработка методов противодействия им; осуществление сбора, обработки, анализа и систематизации научно-технической информации по теме исследования; приобретение практических навыков в оформлении научно-технических отчетов, обзоров и подготовке публикаций по результатам выполненных исследований.	
Результаты освоения дисциплины	Подбирает технологии поиска и критического анализа информации с использованием методов системного подхода Принимает обоснованные стратегические решения на основе анализа нормативно-методически документов Решает поставленные задачи с помощью цифровых и информационных технологий, организует личное цифровое пространство Руководствуется основными законами экономического и финансового развития государства, при стратегическом и тактическом планировании, использует финансовые инструменты в профессиональной деятельности и личных целях руководствуется научными методами, при проведении личного экономического и финансового планирования в целях получения наибольшего эффекта контролирует собственные экономические и финансовые риски, применяя современные информационные технологии и рекомендации ведущих экономистов Предоставляет отчет с детальным анализом назначения системного программного обеспечения, а также структуры операционной системы, предназначения основных параметров и компонентов операционной системы семейства Windows; методов инсталляции системного программного обеспечения, а также режимов его взаимодействия с операционной системой; методов мониторинга компонентов операционной системы Windows, а также режимов отказоустойчивой конфигурации. Предоставляет детальный отчет с результатами установки и удаления операционной системы семейства Windows, развертывания службы каталогов Windows, а также настройки роли сервера; установки и удаления системного программного обеспечения, запуска, остановки и настройки службы Windows. А также результатами использования программного маршрутизатора на базе ОС Windows; диагностики причин сбоев работоспособности операционной системы Windows с помощью системного программного обеспечения. Предоставляет детальный отчет с демонстрацией способности применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности. Разрабатывает и описывает детальный проект по обеспечению информа-	

	ционной безопасности согласно нормативно-правовым механизмам лицензирования, сертификации и аттестации; принципам организационного обеспечения информационной безопасности; основным документам по обеспечению режима и конфиденциальности на объекте; основным документам, регламентирующим организационную безопасность на объекте. Учитывая основные угрозы информационной безопасности на объекте (в организации); порядок организации службы безопасности на объекте; типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; роль персонала в обеспечении информационной безопасности на объекте; основы организационной защиты информации, ее современные проблемы и терминологию. Разрабатывает и описывает детальный проект с эффективным применением знаний теории и методик курса при раскрытии компьютерных преступлений, при работе с конфиденциальной информацией и государственной тайной, при работе с организационно-правовым обеспечением, при работе с ЭП, при защите авторского и международного права, при проведении экспертизы преступлений в сфере компьютерной информации. Проект должен соответствовать нормативно-правовым актам по защите информации. Предоставлен отчет с детальным анализом и оценкой состояния организационной защиты информации на объекте. Предоставляет детальный отчет с демонстрацией способности при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Разрабатывает детально проработанный проект, в котором придерживается последовательности и содержания этапов построения компьютерных сетей; эталонной модели взаимодействия открытых систем; принципов построения и функционирования систем и сетей передачи информации; типовых структур и принципов организации компьютерных сетей; примеров реализации современных локальных и глобальных компьютерных сетей; основных телекоммуникационных протоколов; перспектив развития компьютерных сетей. Предоставляет детальный отчет с демонстрацией способности пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; разрабатывать сетевые проекты с использованием базовых технологий; - оценивать работоспособность сетевых проектов; исследовать характеристики сетевой активности созданных проектов. Предоставляет детальный отчет с демонстрацией способности решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации. Предоставляет детальный отчет с описанием операционных систем; критериев оценки эффективности и надежности средств защиты операционных систем; принципов организации и структуры подсистем защиты операционных систем семейства UNIX и Windows; функций операционных систем, основных концепций управления процессорами, памятью, вспомогательной памятью, устройствами. Предоставляет детальный отчет с демонстрацией способности использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эф-
--	--

	фективность и надёжность защиты операционных систем; планировать политику безопасности операционных систем. Предоставляет детальный отчёт с демонстрацией способности применять знания в области безопасности операционных систем при разработке автоматизированных систем. Предоставляет детальный отчёт с анализом основных угроз информационной безопасности предприятия (организации); методов восстановления работоспособности средств защиты информации при возникновении нештатной ситуации; основных действий сотрудника информационной безопасности предприятия (организации) при возникновении либо обнаружении следов компьютерных преступлений; методов расследования компьютерных преступлений и инцидентов. Предоставляет детальный отчёт с демонстрацией способности проводить диагностику компьютерной системы на обнаружение программно-аппаратных средств совершения киберпреступлений; выявлять следы совершения компьютерных преступлений и проведению оценки защищённости компьютерной системы на защиту информации. Предоставляет детальный отчёт с демонстрацией способности организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов. Предоставляет детальный отчёт с описанием требования по безопасности, предъявляемые к разрабатываемому программному обеспечению. Предоставляет детальный отчёт с описанием основные угрозы безопасности информации и модели нарушителя в информационных системах. Предоставляет детальный отчёт с демонстрацией способности реализовывать план внедрения процесса разработки безопасного программного обеспечения
Трудоемкость, з.е.	3
Формы отчетности	Зачет с оценкой
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Суворова, Г. М. Информационная безопасность Электронный ресурс : Учебное пособие / Г. М. Суворова. - Саратов : Вузовское образование, 2019. - 214 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-4487-0585-4, экземпляров неограничено
Дополнительная литература	1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. http://www.iprbookshop.ru/52209.html 2. Мэйволд Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 571 с. http://www.iprbookshop.ru/73727.html