Аннотации рабочих программ дисциплин

образовательной программы высшего образования.

Направление подготовки «10.04.01 Информационная безопасность», направленность / профиль образовательной программы «Безопасность компьютерных систем»

1. Аннотации рабочих программ дисциплин (модулей) базовой части

Б1.Б.01 Сертификация средств защиты информации

Цели освоения дисциплины

Целью преподавания дисциплины «Сертификация средств защиты информации» является:
изучение студентами способов сертификации средств защиты информации.

Место дисциплины в структуре ОП

Дисциплина «Сертификация средств защиты информации» Б1.Б.01 является одной из дисциплин базовой части учебного плана подготовки магистратуры по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Технологии обеспечения информационной безопасности».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК-1)
– способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3)
– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6)
– способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)
– способностью проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10)
– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15)

– Проведение экспериментальных исследований уровней защищенности компьютерных сетей и систем (ПС-10)

Содержание дисциплины

Раздел 1. Телекоммуникации и их регулирование в правовой системе РФ.
Система норм права, регулирующих деятельность телекоммуникаций в РФ. Субординация норм права. Коллизии права. Конституционные основы деятельности в телекоммуникациях РФ.
Раздел 2. Правовые основы деятельности связи в РФ.
Федеральная связь РФ и ее состав. Сеть связи общего пользования. Выделенные сети связи. Технологические сети связи. Сети связи специального назначения. Государственное регулирование деятельности в области связи. Обязанности операторов связи в соответствии с федеральным законом РФ "О связи". Универсальные услуги связи. Подача жалоб и предъявление претензий и их рассмотрение. Место предъявления претензий. Управление сетями связи в чрезвычайных ситуациях и в условиях чрезвычайного положения. Основные положения Устава и Конвенции Международного союза электросвязи.
Раздел 3. Информация, информационные технологии и защита информации в правовой системе РФ
Информация, информационные технологии, доступ к информации, предоставление информации, распространение информации в соответствии с законом РФ "Об информации, информационных технологиях и о защите информации". Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации в РФ. Виды информации в зависимости от категории доступа и в зависимости от порядка ее предоставления или распространения. Право на доступ к информации. Ограничение доступа к информации. Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав. Защита информации в соответствии с законом РФ "Об информации, информационных технологиях и о защите информации". Обязанности организатора распространения информации в сети "Интернет". Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
Раздел 4. Государственная тайна в РФ.
Перечень сведений, составляющих государственную тайну в РФ. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию в РФ. Допуск должностных лиц и граждан к государственной тайне. Особый порядок допуска к государственной тайне. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне. Условия прекращения допуска должностного лица или гражданина к государственной тайне. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Ответственность за разглашение государственной тайны в РФ.
Раздел 5. Правовая защита персональных данных в РФ.
Персональные данные, их обработка, распространение, предоставление, блокирование, уничтожение и обезличивание в соответствии с федеральным законом РФ "О персональных данных". Принципы обработки персональных данных. Согласие субъекта персональных данных на обработку его персональных данных. Требования, являющиеся обязательными к письменной форме согласия субъекта персональных данных на обработку его персональных данных. Специальные категории персональных данных и перечень оснований для их обработки. Дисциплинарная, административная и уголовная

ответственность за нарушение законодательства РФ о персональных данных.
Раздел 6. Правовое регулирование в РФ информации, причиняющей вред здоровью и (или) развитию детей
Виды информации, причиняющей вред здоровью и (или) развитию детей. Классификация информационной продукции в соответствии с федеральным законом РФ "О защите детей от информации, причиняющих вред их здоровья и развитию".

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.02 Технологии обеспечения информационной безопасности

Цели освоения дисциплины

Целью преподавания дисциплины «Технологии обеспечения информационной безопасности» является:
изучение студентами сущности, содержания и особенностей технологий обеспечения информационной безопасности для больших данных (Big Data)

Место дисциплины в структуре ОП

Дисциплина «Технологии обеспечения информационной безопасности» Б1.Б.02 является одной из дисциплин базовой части учебного плана подготовки магистратуры по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Управление информационной безопасностью»; «Управление информационной безопасностью».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2)
– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2)

– способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5)
– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации (ПС-1)
– Проведение контрольных проверок эффективности применяемых программно-аппаратных средств защиты информации (ПС-2)

Содержание дисциплины

Раздел 1. Введение
Цели и задачи освоения дисциплины. Содержание дисциплины. Принципы и методы изучения дисциплины.
Раздел 2. Большие данные (Big Data)
Основные механизмы работы Big Data, принципиальные отличия от классических систем управления базами данных (СУБД).
Раздел 3. Принципы организационного проектирования систем Big Data.
Рассмотрение основных моделей обработки больших данных, основных наиболее распространенных решений в сфере информационной безопасности на основе Big Data.
Раздел 4. Работа с Big Data
Рассмотрение стандартных механизмов сбора и анализа неструктурированной информации, а также обработка полученных данных из этой информации.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.03 Управление информационной безопасностью

Цели освоения дисциплины

Целью преподавания дисциплины «Управление информационной безопасностью» является:
изучение вопросов управления информационной безопасностью. Дисциплина «Управление информационной безопасностью» должна обеспечивать

формирование фундамента подготовки будущих специалистов в области формирования моделей угроз, оценки рисков информационных инфокоммуникационных систем, формирование адекватных методов и средств обеспечения информационной безопасности, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана. Она должна способствовать развитию творческих способностей студентов, умению формулировать и решать задачи изучаемой специальности, умению творчески применять и самостоятельно повышать свои знания.

Место дисциплины в структуре ОП

Дисциплина «Управление информационной безопасностью» Б1.Б.03 является одной из дисциплин базовой части учебного плана подготовки магистратуры по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Методы и средства защиты электронного документооборота».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью к абстрактному мышлению, анализу, синтезу (ОК-1)
– способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1)
– способностью организовать управление информационной безопасностью (ПК-13)
– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Формирование политик информационной безопасности (ПС-3)
– Разработка требований по защите компьютерных сетей и систем (ПС-4)
– Оценка рисков угроз и соответствия требованиям нормативных документов информационной безопасности (ПС-7)
– Проведение анализа безопасности компьютерных систем (ПС-8)

Содержание дисциплины

Раздел 1. Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика
Организационно-правовые формы управления безопасностью. Предпосылки развития

государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.
Раздел 2. Основные принципы построения SIEM
Средства визуализации элементов ИБ. Визуализация статистики по инцидентам ИБ. Комплексные системы мониторинга ИБ. Средства сбора отчетов и Logов. Основные принципы работы SIEM систем. Составление отчетов по ИБ.
Раздел 3. Проведение комплекса процедур цифрового расследования в информационных и компьютерных системах
Digital Forensic. Расследование инцидентов. Утилиты для расследования инцидентов. Информация об истории посещения сайтов, кукисах, букмарках, скачанных файлах, заполненных формах, сохраненных логинах и т.д.
Раздел 4. Введение в оценку и аудит ИБ путем выявления угроз ИБ «на лету»
Введение в «этический хакинг». Основные принципы его организации. Составление плана проведения тестирования целевой системы (инфраструктуры). Отношение к законодательству и регуляторам. Составление отчета и рекомендаций на основе проведенного тестирования.
Раздел 5. Аудит систем удаленного и локального доступа
Основные механизмы и принципы проведения аудита ИБ СКУД предприятия, а также систем удаленного доступа с использованием технологий виртуальных частных сетей
Раздел 6. Аудит инфраструктуры ИБ, интегрированных сервисов телефонии и беспроводного доступа
Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия. Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии, а также систем беспроводного доступа Wi-Fi
Раздел 7. Принципы организации аудита систем информационной безопасности
Основные техники проведения аудита систем ИБ. Разработка методики проведения аудита систем ИБ. Основные средства проведения аудита систем ИБ.
Раздел 8. Принципы построения интегрированных систем информационной безопасности
Создание политик ИБ предприятия. Принципы обеспечения безопасности инфраструктуры. Принципы обеспечения безопасности периметра сети телекоммуникационной системы. Регулирование правил работы СКУД. Регулирование правил удаленного доступа средствами VPN. Контроль безопасности конечных устройств. Контроль безопасности IP-телефонии.
Раздел 9. Стандарты управления информационной безопасностью
Государственные стандарты в области ИБ РФ. Оценочные стандарты в информационной безопасности. Оранжевая книга. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"
Раздел 10. Оценка рисков информационной безопасности
Основные составляющие информационной безопасности. Угрозы информационной безопасности в информационных системах. Основные определения и критерии, угрозы целостности и конфиденциальности.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.Б.04 Защищенные информационные системы

Цели освоения дисциплины

Целью преподавания дисциплины «Защищенные информационные системы» является:

Целью курса «Защищенные информационные системы» является изучение теоретических и практических основ обеспечения информационной безопасности закрытых и открытых контуров компьютерных систем инфокоммуникационных инфраструктур. В результате изучения дисциплины у студентов должны сформироваться знания, умения и практические навыки, позволяющие разрабатывать политику информационной безопасности объектов защиты и организационно-практические меры по его защите.

Место дисциплины в структуре ОП

Дисциплина «Защищенные информационные системы» Б1.Б.04 относится к базовой части программы магистратуры «10.04.01 Информационная безопасность».
Изучение дисциплины «Защищенные информационные системы» основывается на базе знаний, умений и компетенций, полученных студентами на предыдущем уровне образования.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК-2)
– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– Формирование политик информационной безопасности (ПС-3)

Содержание дисциплины

Раздел 1. Информационная система как объект защиты
Тема 1.1. Эволюция архитектур информационных систем. Тема 1.2. Политика информационной безопасности объекта защиты. Описание объекта защиты. Определение основных приоритетов информационной безопасности. Тема 1.3. Анализ рисков. Формирование перечня критичных ресурсов. Модели нарушителя и угроз.
Раздел 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем
Тема 2.1. Общие требования построения защищенной информационной системы. Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Тема 2.2. Требования к подсистеме аутентификации и управления доступом. Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты. Тема 2.4. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды. Тема 2.5. Требования к средствам построения защищенных виртуальных сетей (VPN) и управления безопасностью.
Раздел 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности
Тема 3.1. Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»:методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели ВОС.Протокол формирования защищенного туннеля на канальном уровне PPTP (Point-to-PointTunnelingProtocol). Протокол формирования защищенного туннеля на канальном уровне L2F (Layer-2 Forwarding). Протокол формирования защищенного туннеля на канальном уровне L2TP (Layer-2 TunnelingProtocol). Общее описание стека протоколов защиты межсетевого уровня IPsec (InternetProtocolSecurity). Протокол обмена ключевой информацией IKE (InternetKeyExchange). Протокол аутентифицирующего заголовка (AuthenticationHeader, AH). Протокол инкапсулирующей защиты содержимого (EncapsulatingSecurityPayload, ESP). Тема 3.2. Технические решения по защите межсетевого взаимодействия и передачи информации. Средства криптографической защиты информации. Тема 3.3. Технические решения по защите от вредоносного кода. Тема 3.4. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и реализации подсистемы аутентификации и идентификации

Общая трудоемкость дисциплины

108 час(ов), 3 ЗЕТ

Форма промежуточной аттестации

Зачет

Б1.Б.05 Технологии обеспечения информационной безопасности больших данных

Цели освоения дисциплины

Целью преподавания дисциплины «Технологии обеспечения информационной безопасности больших данных» является:
студентами сущности, содержания и особенностей технологий обеспечения

информационной безопасности для больших данных (Big Data)

Место дисциплины в структуре ОП

Дисциплина «Технологии обеспечения информационной безопасности больших данных» Б1.Б.05 относится к базовой части программы магистратуры «10.04.01 Информационная безопасность».
Изучение дисциплины «Технологии обеспечения информационной безопасности больших данных» основывается на базе знаний, умений и компетенций, полученных студентами на предыдущем уровне образования.

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК-2)
– способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1)
– способностью проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9)
– способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12)

Содержание дисциплины

Раздел 1. Введение
Цели и задачи освоения дисциплины. Содержание дисциплины. Принципы и методы изучения дисциплины.
Раздел 2. Большие данные (Big Data)
Основные механизмы работы Big Data, принципиальные отличия от классических систем управления базами данных (СУБД).
Раздел 3. Принципы организационного проектирования систем Big Data.
Рассмотрение основных моделей обработки больших данных, основных наиболее распространенных решений в сфере информационной безопасности на основе Big Data.
Раздел 4. Работа с Big Data
Рассмотрение стандартных механизмов сбора и анализа неструктурированной информации, а также обработка полученных данных из этой информации.

Общая трудоемкость дисциплины

180 час(ов), 5 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

2. Аннотации рабочих программ дисциплин (модулей) вариативной части

Б1.В.01 Защита облачных вычислений и телекоммуникаций

Цели освоения дисциплины

Целью преподавания дисциплины «Защита облачных вычислений и телекоммуникаций» является:
изучение принципов построения программно-конфигурируемых сетей, защиты облачных вычислений, принципов работы гипервизора.

Место дисциплины в структуре ОП

Дисциплина «Защита облачных вычислений и телекоммуникаций» Б1.В.01 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Защита облачных вычислений и телекоммуникаций»; «Управление информационной безопасностью».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2)
– Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации (ПС-1)
– Разработка требований по защите компьютерных сетей и систем (ПС-4)
– Разработка средств защиты информации (ПС-5)
– Проведение анализа безопасности компьютерных систем (ПС-8)

Содержание дисциплины

Раздел 1. Введение в сети следующего поколения
Рассматривается переход на сети будущего. Проведено сравнение существующих сетей и сетей будущего.
Раздел 2. Безопасность и защита в облачных вычислениях
Общие понятия облачных вычислений, проблемы обеспечения безопасности облачных вычислений, методология облачных вычислений
Раздел 3. Виртуализация: Проблемы. Угрозы. Решения.
Проблемы виртуализации. Свойства и подходы в виртуализации, угрозы, решения.
Раздел 4. Принципы SDN. Протокол Openflow.
Программно-конфигурируемые сети, структура контроллера SDN, примеры конфигурации на решении компании Cisco Systems. Рассматриваются принципы конфигурирования протокола OpenFlow.
Раздел 5. Виртуализация сетей
Принципы организации виртуальных сетей (на примере vSwitch от VMware), overlay сети.
Раздел 6. Виртуальные частные сети. Сетевой уровень. Транспортный уровень (протокол SSL/TLS)
Рассматриваются все современные методы создания VPN, включая такие методы, как: IPsecVTI, динамические VTI, GETVPN, DMVPN, FlexVPN. Рассматриваются структуры протоколов IPsec, IKEv.1 ив.2, приведены сравнительные характеристики всех современных методов построения VPN. Рассматриваются протоколы построения шифрованных туннелей трафика SSL/TLS. Приводятся основные уязвимости протоколов и способы борьбы с ними.
Раздел 7. Защита контроллера SDN
Рассматриваются принципы организации защиты SDN контроллера, на примере компании Cisco Systems.
Раздел 8. Системы детекции/предотвращения вторжений и аномалий
Рассматриваются системы предотвращения вторжений и аномалий (на примере ПО с открытым исходным кодом – Snort)
Раздел 9. Защита OpenStack
Рассматривается комплекс проектов свободного программного обеспечения, который может быть использован для создания инфраструктурных облачных сервисов и облачных хранилищ, как публичных, так и частных
Раздел 10. Настройка продвинутого NAT, фаервола следующего поколения
Приводятся конфигурации и принцип действия фаерволов следующего поколения (NGFW)
Раздел 11. Конфиденциальность облачных вычислений. Целостность облачных вычислений
Приводятся основные угрозы и стратегии защиты облачных вычислений.
Рассматриваются основные угрозы целостности данных и методы защиты от угроз в облачных вычислениях.

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

Б1.В.02 Тестирование на проникновение и этичный хакинг

Цели освоения дисциплины

Целью преподавания дисциплины «Тестирование на проникновение и этичный хакинг» является:
изучение методов анализа угроз корпоративной сети

Место дисциплины в структуре ОП

Дисциплина «Тестирование на проникновение и этичный хакинг» Б1.В.02 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Разработка защищенных приложений».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9)
– способностью проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10)
– Проведение контрольных проверок эффективности применяемых программно-аппаратных средств защиты информации (ПС-2)
– Оценка рисков угроз и соответствия требованиям нормативных документов информационной безопасности (ПС-7)

Содержание дисциплины

Раздел 1. Сканирование и рекогносцировка в сетевой IP-инфраструктуре
Основные методы идентификации устройств в IP-сети, программное обеспечение для проведения идентификации. Сканирование сетевой инфраструктуры и определение топологии сети
Раздел 2. Эксплуатация уязвимостей операционных и SCADAсистем
Основные методы поиска уязвимостей операционных систем (Windows, Linux, MacOS). Методы эксплуатации уязвимостей. Использование п/о rootkits, keylogger. Эксплуатация уязвимостей файловых систем и подсистем ввода/вывода информации. Основы поиска

уязвимостей SCADA-систем
Раздел 3. Перехват трафика
Основные методы перехвата трафика на канальном и сетевом уровне, в соответствии со стеком протоколов TCP/IP. Эксплуатация уязвимостей типа подмены MAC, IP-адресов. Атаки на ARPпротокол. Основное п/о для эксплуатации уязвимостей такого типа.
Раздел 4. Отказы в обслуживании
Проведение атак типа «Отказ в обслуживании» и «Распределенный отказ в обслуживании». Основное п/о для проведения атак такого типа. Принципы атак такого типа.
Раздел 5. Перехват сессий и сетевых соединений
Основные методы поиска уязвимостей в реализации протоколов сетевого и транспортного уровней, в соответствии со стеком протоколов TCP/IP. Методы эксплуатации уязвимостей такого типа. Перехват соединений TCP. Основное п/о для эксплуатации уязвимостей такого типа.
Раздел 6. Эксплуатация уязвимостей WEB-сервисов и приложений
Основные методы поиска и эксплуатации уязвимостей WEB-сервисов (HTTP)и WEB-приложений (с использование языков программирования Java, PHP). Исследование SQL-инъекций.
Раздел 7. Поиск и эксплуатация уязвимостей беспроводных сетей, работающих по стандарту 802.11
Основные методы поиска и эксплуатации уязвимостей беспроводных сетей Wi-Fi. Основные уязвимости в протоколах безопасности WEP, WPA/WPA2. П/о для эксплуатации уязвимостей такого типа.
Раздел 8. Поиск уязвимостей в мобильных устройствах
Основные методы поиска и эксплуатации уязвимостей в мобильных устройствах, в том числе эксплуатация уязвимостей персональных беспроводных сетей Bluetooth, ZigBee.
Раздел 9. Методы обхода систем предотвращения вторжений и межсетевых экранов
Основные методы поиска и эксплуатации уязвимостей в работе систем предотвращения вторжений и межсетевых экранов. Программное обеспечение, позволяющее эксплуатировать уязвимости такого типа
Раздел 10. Использование вирусов, закладок в коде. Переполнение буффера
Основные методы использования вредоносного п/о при проведении анализа уязвимостей инфокоммуникационных систем. Использование ошибок в программном коде для проведения атак типа «Переполнение буффера».
Раздел 11. Поиск уязвимостей в реализациях криптографических алгоритмов
Основные методы эксплуатации уязвимостей реализованных криптографических алгоритмов для проведения атак на виртуальные частные сети.
Раздел 12. Методы сокрытия деятельности в сети.
Основные методы анонимизации присутствия в цифровом пространстве и методы сокрытия деятельности, связанной с сетевой активностью

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен

Б1.В.03 Разработка защищенных приложений

Цели освоения дисциплины

Целью преподавания дисциплины «Разработка защищенных приложений» является:

изучение принципов построения безопасного кода на языке программирования Java, использования и разработки собственных функций обеспечения информационной безопасностью.

Место дисциплины в структуре ОП

Дисциплина «Разработка защищенных приложений» Б1.В.03 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность».
Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Защита облачных вычислений и телекоммуникаций».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2)
– способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12)
– способностью организовать управление информационной безопасностью (ПК-13)
– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– Формирование политик информационной безопасности (ПС-3)
– Разработка требований по защите компьютерных сетей и систем (ПС-4)
– Разработка средств защиты информации (ПС-5)

Содержание дисциплины

Раздел 1. Введение в Java
Язык Java как средство программирования, преимущества, характерные особенности. Язык Java и Интернет. Отличия от C++. Типы данных, арифметические, логические, условные операторы и операторы цикла. Одномерные и многомерные массивы. Примеры простых программ.
Раздел 2. Основы объектно-ориентированного программирования
Введение в концепцию объектно-ориентированного программирования, основные

понятия, особенности реализации. Объявления классов. Основные компоненты класса: поля, методы, конструкторы. Вводится понятие наследования, полиморфизма. Обобщённые типы данных.Общие сведения об исключениях, обработка исключений с помощью конструкции try/catch/finally.Создание собственного исключения. Алгоритм обработки ошибок.
Раздел 3. Потоки ввода-вывода
Ввод-вывод данных в консольном и графическом режиме.форматирование вывода, считывание ввода. Работа с потоками. Работа с текстовыми и бинарными файлами. Работа с сетью TCP/IP. Многопоточное программирование
Раздел 4. Графический интерфейс
Создание окон, кнопок на окне, полей вывода, ввода, поля для рисования. Включение скроллинга. Менеджеры компоновки.
Раздел 5. Обработка событий
Знакомство с методами обработки событий в Java: нажатие кнопки, движение мыши, нажатию кнопки на клавиатуре и д.р. с помощью интерфейсов.
Раздел 6. Структура байт кода
Компиляция .javав .class., структура файла .class: заголовок; пул констант; объявления класса; поля методы; имена типов, методов и классов; исполняемый код. Примеры соответствия кода и байт кода
Раздел 7. Основные механизмы обеспечения безопасности
Введение в основные механизмы встроенные в виртуальную машину JRE: загрузчики классов, верификация байт кода, диспетчеры полномочий, аутентификация пользователей, цифровые подписи, цифровые сертификаты, алгоритмы шифрования.
Раздел 8. Цифровые водяные знаки в исполнимых файлах
Введение в основы вложения сообщений в исполняемый код. Рассмотрены особенности вложение в отличие от классических покрывающих сообщений. Применение вложений в качестве цифровых водяных знаков.

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

Б1.В.04 Технологии защиты беспроводных сетей и мобильных приложений

Цели освоения дисциплины

Целью преподавания дисциплины «Технологии защиты беспроводных сетей и мобильных приложений» является:
изучение методов анализа угроз корпоративной сети

Место дисциплины в структуре ОП

Дисциплина «Технологии защиты беспроводных сетей и мобильных приложений» Б1.В.04 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Защита сетевых приложений».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1)
– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2)
– способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3)
– Разработка средств защиты информации (ПС-5)
– Разработка требований по защите информации беспроводных и мобильных компьютерных сетей (ПС-6)

Содержание дисциплины

Раздел 1. Введение в администрирование VMware
Общие принципы работы виртуальной машины.
Раздел 2. Администрирование систем хранения данных (СХД)
Работа с разделами Virtual Machine File Systems (VMFS). Storage VMotion.
Раздел 3. Конфигурирование сети
Настройка и безопасность виртуальных сетей. Настройка программного адаптера iSCSI. Настройка брендмауэра Service Console.
Раздел 4. Введение в разработку Android-приложений»
Краткая история ОС Android. Intel для Android: партнерство и инструментарий разработчика. Архитектура приложений для Android. Ресурсы приложения. Пользовательский интерфейс. Инструментарий разработки приложений для Android. Обзор шагов разработки типичного приложения под Android. Особенности разработки с использованием эмулятора. Отладка кода в эмуляторе и на реальных приложенийах.
Раздел 5. Создание пользовательских интерфейсов и использование элементов управления в приложениях под Android»
Текстовые элементы управления, кнопки, списки, таблицы, управление датой и временем, MapView, галерея, счетчик, диспетчеры шаблонов, адаптеры, создание меню, 8 расширенные меню, загрузка меню при помощи XML-файлов, создание диалоговых окон, диалоговые окна с подсказками и предупреждениями.
Раздел 6. 2D-анимация, создание и использование служб в приложениях под Android»
Планирование покадровой анимации, анимирование, анимация шаблонов, видов, использование класса Camera. Проверка безопасности, работа со службами, основанными

на местоположении, использование HTTP-служб, службы AIDL
Раздел 7. Работа с Android Market
Подготовка AndroidManifest.xml для закачки, локализация приложения, подготовка ярлыка приложения, подготовка APK-файла для закачки, работа пользователя с Android Market
Раздел 8. Инструменты Intel для оптимизации и отладки Android-приложений
Intel Power Monitoring Tool. Intel Graphics Performance Analyzer. Intel Energy Checker SDK. Intel Hardware Accelerated Execution Manager.

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовой проект

Б1.В.ДВ.01.01 Цифровая криминалистика

Цели освоения дисциплины

Целью преподавания дисциплины «Цифровая криминалистика» является: изучение основ расследования инцидентов информационной безопасности.

Место дисциплины в структуре ОП

Дисциплина «Цифровая криминалистика» Б1.В.ДВ.01.01 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Тестирование на проникновение и этичный хакинг».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5)
– способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6)

– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)
– Проведение сертификации программно-аппаратных средств защиты информации (ПС-9)

Содержание дисциплины

Раздел 1. Введение в цифровые доказательства
Значение термина цифровой форензики, стандартные процедуры, методы написания отчетов, технологии документирования, стандарты для идентификации, сбора информации (ISO/IEC 27037), описание инструментов с кратким анализом функционала xmount, guymager, ewf-tools, и т.д., настройка рабочей станции.
Раздел 2. Работа с данными
Создание образа для цифровой форензики: описание инструментария, команды Linux, форматы образов (dd, ewf), хеширование (контроль за целостностью данных – функции MD5, SHA1, SHA256)..
Раздел 3. Работа с жесткими дисками.
Физические и логические тома, функции: образы для разбиения дисков, MBR, GPT, обзорфункций RAID-массивов.
Раздел 4. Файловые системы
FAT, основные функции NTFS, основные функции HFS and HFS+
Раздел 5. Анализ работы операционных систем на примере семейства ОС Windows
Анализ логов ОС Windows, конфигурационного регистра, браузеров, метаданных.
Раздел 6. Анализ интернет приложений ОС Windows
Браузеры, мессенджеры, p2p приложения, инструментарии для анализа приложений Windows (sqllite-bowser), шифрование (bitlockers).
Раздел 7. Анализ уязвимостей ОС Linux, MacOS
Анализ логов, истории активности пользователей, конфигурация
Раздел 8. Анализ уязвимостей MacOS
Анализ логов, истории активности пользователей, конфигурация.
Раздел 9. Сетевая форензика
Перехват сетевого трафика, анализ уровня приложений, инструментарий для сетевой форензики (Wireshark, Ettercap, другие).
Раздел 10. Форензика в реальном времени
Обслуживание машин в реальном времени, функции данных в реальном времени на примере ОС Windows, Linux, Mac OS).
Раздел 11. Форензика SSD
Инструментарии для работы с форензикой SSD, функциональные особенности
Раздел 12. Форензика памяти
Основы работы с анализом памяти, аналитика дампов памяти RAM

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

Б1.В.ДВ.01.02 Основы стеганографии

Цели освоения дисциплины

Целью преподавания дисциплины «Основы стеганографии» является: изучение студентами особенностей применения стеганографии и предъявляемых к ней требования. Дисциплина «Основы стеганографии» должна обеспечивать формирование фундамента подготовки будущих специалистов в области защиты авторских прав, обеспечения целостности передаваемой или сохраняемой информации на носителях с помощью стеганографических методов защиты информации, а также, создавать необходимую базу для успешного овладения последующими специальными дисциплинами учебного плана.

Место дисциплины в структуре ОП

Дисциплина «Основы стеганографии» Б1.В.ДВ.01.02 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Защищенные информационные системы».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5)
– способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6)
– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)
– Проведение сертификации программно-аппаратных средств защиты информации (ПС-9)

Содержание дисциплины

Раздел 1. Области применения стеганографии
Определение цифровой стеганографии (СГ) в широком смысле. Собственно СГ и цифровые “водяные” знаки (ЦВЗ).Типичные покрывающие сообщения (ПС).Основные атаки на системы СГ и ЦВЗ.
Раздел 2. Простейшие системы СГ
Вложение в наименьшие значащие биты (НЗБ) с замещением и НЗБ с согласованием. Основные свойства СГ-НЗБ. Примеры систем с НЗБ (Jsteg,Outgiess,F5). СГ, использующие широкополосные сигналы (СГ-ШПС) и их свойства. Слепой и информированный декодеры.
Раздел 3. СГ для других покрывающих сообщений
Лингвистические, графические, Интернет СГ и их свойства.
Раздел 4. СГ стойкие к оптимальному статистическому обнаружению
Критерии секретности СГ.Относительная энтропия. Модельно обусловленные СГ.СГ на основе адаптивного квантования. СГ с сохранением статистики ПС. Слепой стегоанализ.
Раздел 5. Общие сведения о системах с ЦВЗ
Классификация систем ЦВЗ. Основные атаки на системы ЦВЗ. Критерии эффективности ЦВЗ. Виды ПС использующихся с ЦВЗ. Основные применения систем ЦВЗ
Раздел 6. Техника погружения и извлечения ЦВЗ устойчивых к случайному и преднамеренному удалению
Классификация систем ЦВЗ. Основные атаки на системы ЦВЗ. Критерии эффективности ЦВЗ. Виды ПС использующихся с ЦВЗ. Основные применения систем ЦВЗ (мониторинг рекламы ,идентификация пользователей доказательство прав собственности, аутентификация ПС).
Раздел 7. Особенности построения систем ЦВЗ для аудио и видео сигналов
ЦВЗ на основе использования явлений эхо и реверберации. Применение кепстральных методов в декодере. Защита от преобразований форматов. Основные методы построения систем ЦВЗ для видео ПС различных стандартов.

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

Б1.В.ДВ.02.01 Вредоносное программное обеспечение

Цели освоения дисциплины

Целью преподавания дисциплины «Вредоносное программное обеспечение» является:

изучение вопросов основ защиты информации в глобальной сети на основе антивирусных решений компании ESET NOD32, одного из лидеров в этой области разработки антивирусного программного обеспечения.

Место дисциплины в структуре ОП

Дисциплина «Вредоносное программное обеспечение» Б1.В.ДВ.02.01 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Разработка защищенных приложений».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Проведение анализа безопасности компьютерных систем (ПС-8)
– Проведение экспериментальных исследований уровней защищенности компьютерных сетей и систем (ПС-10)

Содержание дисциплины

Раздел 1. Компьютерные угрозы, основная классификация вредоносного ПО
Эволюция программ с вредоносным ПО, примеры
Раздел 2. Технологии атак, архитектура x86
Технологии атак, архитектура x86
Раздел 3. Фишинговые атаки, угрозы онлайн банкинга
Определение и классификация фишинговых атак, детекция атак, обзор угроз онлайн банкинга, примеры атак, методы защиты
Раздел 4. Программное обеспечение, предназначенное для вымогательства
Классификация угроз Ransom ware and Scareware. Примеры атак, методы защиты от угроз.
Раздел 5. Ботнеты
Определение, топологии, протоколы взаимодействия, примеры.
Раздел 6. Угрозы мобильных платформ: IOS
Классификация основных видов угроз IOS. Вирусы и уязвимости AppleIOS. Средства защиты.
Раздел 7. Угрозы мобильных платформ: Android
Обзор архитектуры Android. Примеры программ. Патчи, эксплоиты.
Раздел 8. Веб-угрозы, социальная инженерия, угрозы и уязвимости
Понятие уязвимостей и угроз. Web-эксплоиты, PDF, MSOffice, другие.
Раздел 9. Руткиты и буткиты

ОбзорWindows Kernel (ядра ОС Windows), понятие руткитов, эволюция руткитов. Понятие буткитов, эволюция.
Раздел 10. Антивирусные технологии
Определение комплексных антивирусов, классификация, современные антивирусные технологии
Раздел 11. Технологии sandbox
Определение sandbox. Доступные решения на рынке для борьбы с вредоносным ПО
Раздел 12. Определение вредоносного ПО, интеллектуальный анализ данных
Основные средства борьбы с вредоносным ПО, интеллектуальный анализ данных

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

Б1.В.ДВ.02.02 Защита сетевых приложений

Цели освоения дисциплины

Целью преподавания дисциплины «Защита сетевых приложений» является:
Целью изучения дисциплины «Защита сетевых приложений» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий.

Место дисциплины в структуре ОП

Дисциплина «Защита сетевых приложений» Б1.В.ДВ.02.02 является одной из дисциплин цикла учебного плана подготовки магистров по направлению «10.04.01 Информационная безопасность». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как: «Защищенные информационные системы».

Требования к результатам освоения

Процесс изучения дисциплины направлен на формирование следующих компетенций:
В соответствии с ФГОС:

– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Проведение анализа безопасности компьютерных систем (ПС-8)
– Проведение экспериментальных исследований уровней защищенности компьютерных сетей и систем (ПС-10)

Содержание дисциплины

Раздел 1. Методы экспериментов с черным ящиком
Методы экспериментов с черным ящиком; Статический метод; Динамический метод.
Раздел 2. Методы исследования программ
Метод маяков; Метод Step-Trace первого этапа; Метод аппаратной точки останова; Динамическое изменение кода программы; Искусственное усложнение структуры программы; Нестандартное обращение к функциям операционной системы; Искусственное усложнение алгоритмов обработки данных; Выявление фактов выполнения программы под отладчиком.
Раздел 3. Особенности анализа программ
Особенности анализа оверлейновых программ; Особенности анализа графических программ; •Особенности анализа параллельного кода; Особенности анализа кода в режиме ядра Windows.
Раздел 4. Защита программ от анализа
Динамический метод; Искусственное усложнение структуры программы; Искусственное усложнение структуры программы; Искусственное усложнение алгоритмов обработки данных; Выявление факта выполнения программы под отладчиком.
Раздел 5. Модели взаимодействия программной закладки с атакуемой системой
Модель «наблюдатель»; Модель «перехват»; Модель «искажение»; Несанкционированное использование средств динамического изменения полномочий;
Раздел 6. Предпосылки к внедрению программ закладок
Уязвимость переполнения буфера; Уязвимость "отсутствие необходимых проверок входных данных"; GetAdmin;
Раздел 7. Методы внедрения программных закладок
Классификация методов внедрения программных закладок; Маскировка программной закладки под прикладное программное обеспечение; Маскировка программной закладки под системное программное обеспечение;
Раздел 8. Защитные механизмы
Методы защиты; Классификация защит по роду секретного ключа; Надежность защиты; Недостатки готовых "коробочных" решений.
Раздел 9. Распространенные ошибки реализации защитных механизмов
Защита от несанкционированного копирования и распространения серийных номеров; Защита испытательным сроком и ее слабые места; Проблема переустановки; Реконструкция алгоритма; Несколько серийных номеров в одном;

Общая трудоемкость дисциплины

252 час(ов), 7 ЗЕТ

Форма промежуточной аттестации

Экзамен. Курсовая работа

3. Аннотации программ практик

производственной Б2.В.01.01(Н) Научно-исследовательская работа

Цели проведения практики

Целью проведения практики «Научно-исследовательская работа» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;
- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;
- планирование исследования (выбор темы, обоснование необходимости, определение целей и задач, выдвижение гипотез, формирование программы, подбор средств и инструментария);
- проведение исследования (изучение литературы, сбор, обработка и обобщение данных, объяснение полученных результатов и новых фактов, аргументирование, формулировка выводов);
- оформление отчета о результатах исследования (изучение нормативных требований, формирование структуры и содержания, написание, редактирование, формирование списка использованных источников информации, оформление приложений);
- выступление с докладами на студенческих конференциях по результатам исследований.

Место практики в структуре ОП

«Научно-исследовательская работа» Б2.В.01.01(Н) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.04.01 Информационная безопасность».

«Научно-исследовательская работа» опирается на знания полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Преддипломная практика».

Требования к результатам освоения

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2)
– способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1)
– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5)
– способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6)
– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)
– способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12)
– способностью организовать управление информационной безопасностью (ПК-13)
– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации (ПС-1)
– Проведение контрольных проверок эффективности применяемых программно-аппаратных средств защиты информации (ПС-2)

– Формирование политик информационной безопасности (ПС-3)
– Разработка требований по защите компьютерных сетей и систем (ПС-4)
– Разработка требований по защите информации беспроводных и мобильных компьютерных сетей (ПС-6)
– Проведение анализа безопасности компьютерных систем (ПС-8)

Содержание практики

Раздел 1. Согласование темы индивидуального задания
Выбор темы, из списка представленного научным руководителем и последующее согласование
Раздел 2. Составление индивидуального плана работы студента
согласование индивидуального плана работ с научным руководителем
Раздел 3. Выполнение индивидуального задания
Выполнение индивидуального задания
Раздел 4. Подготовка отчета
Предоставление предварительного отчета научному руководителю для согласования
Раздел 5. Защита отчета
Проведение зачета по практике с последующим ответом на вопросы согласно с выбранной теме

Общая трудоемкость дисциплины

756 час(ов), 21 ЗЕТ

Форма промежуточной аттестации

Зачет

производственной Б2.В.01.02(П) Практика по получению профессиональных умений и опыта профессиональной деятельности

Цели проведения практики

Целью проведения практики «Практика по получению профессиональных умений и опыта профессиональной деятельности» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;

- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;

Место практики в структуре ОП

«Практика по получению профессиональных умений и опыта профессиональной деятельности» Б2.В.01.02(П) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.04.01 Информационная безопасность».

«Практика по получению профессиональных умений и опыта профессиональной деятельности» опирается на знания полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Научно-исследовательская работа».

Требования к результатам освоения

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2)
– способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1)
– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2)
– способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3)
– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5)
– способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6)
– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)

– способностью проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9)
– способностью проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10)
– способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12)
– способностью организовать управление информационной безопасностью (ПК-13)
– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации (ПС-1)
– Проведение контрольных проверок эффективности применяемых программно-аппаратных средств защиты информации (ПС-2)
– Формирование политик информационной безопасности (ПС-3)
– Разработка требований по защите компьютерных сетей и систем (ПС-4)
– Разработка средств защиты информации (ПС-5)
– Разработка требований по защите информации беспроводных и мобильных компьютерных сетей (ПС-6)
– Оценка рисков угроз и соответствия требованиям нормативных документов информационной безопасности (ПС-7)
– Проведение анализа безопасности компьютерных систем (ПС-8)
– Проведение сертификации программно-аппаратных средств защиты информации (ПС-9)
– Проведение экспериментальных исследований уровней защищенности компьютерных сетей и систем (ПС-10)

Содержание практики

Раздел 1. Согласование темы индивидуального задания
Выбор и согласование темы с научным руководителем
Раздел 2. Составление индивидуального плана работы студента
определение и согласование индивидуального плана работы
Раздел 3. Выполнение индивидуального задания
получение и выполнение индивидуального задания
Раздел 4. Подготовка отчета
оформление и подготовка работы
Раздел 5. Защита отчета
выступление и защита работы

Общая трудоемкость дисциплины

540 час(ов), 15 ЗЕТ

Форма промежуточной аттестации

Зачет

производственной Б2.В.01.03(Пд) Преддипломная практика

Цели проведения практики

Целью проведения практики «Преддипломная практика» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;
- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;
- подбор необходимых материалов для выполнения выпускной квалификационной работы (или магистерской диссертации).

- Изучить основы написания компьютерных приложений - Изучить документацию к средствам защиты, использующимся на территории РФ - Изучить основы организации систем контроля доступа и видеонаблюдения на режимном объекте - Изучить основные механизмы защиты в телекоммуникационных сетях

Место практики в структуре ОП

«Преддипломная практика» Б2.В.01.03(Пд) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.04.01 Информационная безопасность».

«Преддипломная практика» опирается на знания и практические навыки полученные при изучении дисциплин и прохождении всех типов практик. «Преддипломная практика» является завершающей в процессе обучения и предшествует выполнению выпускной квалификационной работы.

Требования к результатам освоения

В процессе прохождения практики студент формирует и демонстрирует следующие компетенции:

– способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2)
– способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1)
– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2)
– способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3)
– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5)
– способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6)
– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)
– способностью проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9)
– способностью проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10)
– способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12)
– способностью организовать управление информационной безопасностью (ПК-13)
– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации (ПС-1)
– Формирование политик информационной безопасности (ПС-3)
– Разработка требований по защите информации беспроводных и мобильных компьютерных сетей (ПС-6)
– Проведение анализа безопасности компьютерных систем (ПС-8)
– Проведение сертификации программно-аппаратных средств защиты информации (ПС-9)

Содержание практики

Раздел 1. Согласование темы индивидуального задания
Выбор и согласование темы с научным руководителем
Раздел 2. Составление индивидуального плана работы студента
определение и согласование индивидуального плана работы
Раздел 3. Выполнение индивидуального задания
получение и выполнение индивидуального задания
Раздел 4. Подготовка отчета
оформление и подготовка работы
Раздел 5. Защита отчета
выступление и защита работы

Общая трудоемкость дисциплины

540 час(ов), 15 ЗЕТ

Форма промежуточной аттестации

Зачет

4. Аннотация программы ГИА

«Государственная итоговая аттестация»

Цели и задачи дисциплины

Целью государственной итоговой аттестации является определение соответствия результатов освоения студентами основной профессиональной образовательной программы высшего образования требованиям федерального государственного образовательного стандарта (далее ФГОС ВО) по направлению подготовки (специальности) «10.04.01 Информационная безопасность», ориентированной на на следующие виды деятельности:
- проектная
- научно-исследовательская
- контрольно-аналитическая
- организационно-управленческая.

Место дисциплины в структуре ОП

В соответствии с учебным планом государственная итоговая аттестация проводится в конце последнего года обучения. При условии успешного прохождения всех установленных видов итоговых аттестационных испытаний,

входящих в итоговую государственную аттестацию, выпускнику присваивается соответствующая квалификация.

Требования к результатам освоения

Программа ГИА направлена на оценку результатов освоения обучающимися образовательной программы и степени овладения следующими профессиональными компетенциями (ПК):
В соответствии с ФГОС:

– способностью к абстрактному мышлению, анализу, синтезу (ОК-1)
– способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК-2)
– способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК-1)
– способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2)
– способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1)
– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2)
– способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3)
– способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4)
– способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5)
– способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-6)
– способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7)
– способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8)
– способностью проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9)
– способностью проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10)
– способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12)
– способностью организовать управление информационной безопасностью (ПК-13)

– способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14)
– способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15)
– способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности (ПК-16)
– Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации (ПС-1)
– Проведение контрольных проверок эффективности применяемых программно-аппаратных средств защиты информации (ПС-2)
– Формирование политик информационной безопасности (ПС-3)
– Разработка требований по защите компьютерных сетей и систем (ПС-4)
– Разработка средств защиты информации (ПС-5)
– Разработка требований по защите информации беспроводных и мобильных компьютерных сетей (ПС-6)
– Оценка рисков угроз и соответствия требованиям нормативных документов информационной безопасности (ПС-7)
– Проведение анализа безопасности компьютерных систем (ПС-8)
– Проведение сертификации программно-аппаратных средств защиты информации (ПС-9)
– Проведение экспериментальных исследований уровней защищенности компьютерных сетей и систем (ПС-10)

Содержание

Подготовка и защита выпускной квалификационной работы

Общая трудоемкость дисциплины

216 час(ов), 6 ЗЕТ