МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Декан факультета
факультет компьютерных наук

А.А. Крыловецкий

23.04.2024г.

ПРОГРАММА ПРАКТИКИ

Б2.О.06(П) Производственная практика, по получению профессиональных умений и навыков в области профессиональной деятельности

1. Шифр и наименование направления подготовки / специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки / специализация/магистерская программа:
анализ безопасности компьютерных систем

3. Квалификация выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации ФКН

6. Составители программы:
Борисова Алла Александровна, доцент

7. Рекомендована:
Протокол НМС ФКН № 5 от 05.03.2024 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2028/2029 **Семестр(ы):** 10

9. Цель практики:

Целью производственной практики по получению профессиональных умений и опыта профессиональной деятельности является развитие профессиональных знаний и компетенций студентов, получение профессиональных умений и опыта профессиональной деятельности на базе учебных задач, для решения которых необходимо использовать современные информационные технологии обработки и защиты информации.

Задачи практики:

Получение практического опыта работы:

- формирование у студентов умений и навыков проведения технического обследования объекта информационной защиты: сбора экспериментального и экспертного материала и его теоретического обобщения, разработки технических предложений;
- обучение студентов методикам работы с измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач обеспечения информационной безопасности;
- знакомство студентов с методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации.

10. Место практики в структуре ООП:

Базовая часть, блок Б2.

Для успешного прохождения практики студент должен обладать знаниями, умениями и навыками, сформированными в процессе освоения учебных дисциплин: Б1.О.30 Информатика; Б1.О.53.05 Web-технологии; Б1.О.53.06 Алгоритмы и структуры данных; Б1.О.24 Математическая логика и теория алгоритмов; Б1.О.20 Теория вероятностей и математическая статистика; Б1.О.23 Линейная алгебра; Б1.О.31 Информатика; Б1.О.35 Объектно-ориентированное программирование; Б1.О.37 Методы программирования; Б1.О.39 Основы информационной безопасности; Б1.О.40 Модели безопасности компьютерных систем; Б1.О.49 Организационное и правовое обеспечение информационной безопасности; Б1.О.26 Дифференциальные уравнения; Б1.О.51 Защита информации от утечки по техническим каналам; Б1.В.01 Стеганография и цифровые водяные знаки; Б1.О.44 Защита программ и данных; Б1.О.42 Основы построения защищенных компьютерных сетей; Б1.О.43 Основы построения защищенных баз данных; Б1.О.46 Криптографические протоколы; Б1.О.29 Теория информации; Б1.В.02 Моделирование систем; Б1.В.04 Методология экспериментальных исследований и испытаний; Б1.В.05 Анализ уязвимостей программного обеспечения.

В результате прохождения практики, студент должен уметь решать следующие профессиональные задачи:

- Знать правила эксплуатации и особенности применяемого в профильной организации оборудования, уметь работать с действующими стандартами, положениями и инструкциями по деятельности подразделения.
- Знания и умения по установке, настройке, эксплуатация и поддержании в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований, администрирование подсистем информационной безопасности объекта;
- Демонстрировать практический опыт проведения аттестации объектов информатизации по требованиям безопасности информации, аудит информационной безопасности автоматизированных систем, составление

необходимых инструкций, проведение оценки соответствия выполненной работы техническому заданию и действующим нормативным документам.

– Разрабатывать технологическую и эксплуатационную документацию.

– Профессионально взаимодействовать с представителями организаций, представлять презентации результатов технических предложений, подготавливать и оформлять документацию.

11. Вид практики, способ и форма ее проведения

Вид практики: *производственная***.**

Способ проведения практики: *стационарная***.**

Форма проведения практики: *непрерывная.*

12. Планируемые результаты обучения при прохождении практики (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.3 ОПК-5.4 ОПК-5.9 ОПК-5.10 ОПК-5.11 ОПК-5.12 ОПК-5.13 ОПК-5.17 ОПК-5.19	Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав. Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации. Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации. Умеет формулировать основные требования информационной без-	Знать: - основы правовых знаний в различных сферах деятельности; - нормативные правовые акты для профессиональной деятельности; - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требований к защите информации; - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - способы обеспечения защиты и безопасности ИС; - сущность и понятия лицензирования в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации, характеристики их составляющих; Уметь: - использовать правовые знания в различных сферах деятельности; - использовать нормативные правовые акты в профессиональной деятельности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - определять классы защищенности автоматизирован-

			опасности при эксплуатации компьютерной системы. Умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации. Умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам владеет методами и средствами технической защиты информации.	ных систем и средств вычислительной техники, применять методы и средства проектирования программного обеспечения, используемые при создании защищенных компьютерных систем, методы определения требований к защите информации; - проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности. Владеть: - навыками применения правовых знаний в различных сферах деятельности; - навыками применения нормативных правовых актов в профессиональной деятельности; - навыками определения основных характеристик при лицензировании в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств защиты информации; - навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; - международно-правовой терминологией; - навыками работы с международно-правовыми актами, нормативными правовыми актами России; - навыками сравнительного анализа российской модели регулирования информационных отношений с международно-правовыми стандартами и аналогичными институтами зарубежных стран; - практическими навыками использования инструментальных интеллектуальных систем для обоснования требований к защите информации.
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в	ОПК-6.6 ОПК-6.7 ОПК-6.9 ОПК-6.10	Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем. Умеет разрабатывать проекты инструкций,	Знать: - основы правовых знаний в различных сферах деятельности; - нормативные правовые акты для профессиональной дея-

	компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации. Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации. Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	тельности; - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - сущность и понятия лицензирования в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации, характеристики их составляющих; - методы определения требований к защите информации; - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - способы обеспечения защиты и безопасности ИС. Уметь: - использовать правовые знания в различных сферах деятельности; - использовать нормативные правовые акты в профессиональной деятельности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - определять классы защищенности автоматизированных систем и средств вычислительной техники, применять методы и средства проектирования программного обеспечения, используемые при создании защищенных компьютерных систем, методы определения требований к защите информации; - проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности. Владеть: - навыками определения основных характеристик при лицензировании в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств защиты информации;

				- навыками применения правовых знаний в различных сферах деятельности; - навыками применения нормативных правовых актов в профессиональной деятельности; - навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; - международно-правовой терминологией; - навыками работы с международно-правовыми актами, нормативными правовыми актами России; - навыками сравнительного анализа российской модели регулирования информационных отношений с международно-правовыми стандартами и аналогичными институтами зарубежных стран; - практическими навыками использования инструментальных интеллектуальных систем для обоснования требований к защите информации.
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.3 ОПК-9.4 ОПК-9.9 ОПК-9.16 ОПК-9.17	Умеет организовать защиту информации от утечки по техническим каналам на объектах информатизации. Умеет пользоваться нормативными документами в области технической защиты информации. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем. Владеет методами и средствами технической защиты информации. Владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации.	Знать: - принципы формирования политик безопасности для компьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации информационных систем в соответствии с требованиями по защите информации; - математические основы симметричных и асимметричных криптографических систем; - принципы работы симметричных и асимметричных криптографических систем, принципы генерации, хранения и использования криптографических ключей, принципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, современные стандарты шифрования, хеширования, электронной подписи; - основные принципы классификации и количественных характеристик технических каналов утечки информации;

				- основные способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - основы принципов организации защиты информации от утечки по техническим каналам на объектах информатизации; - основные нормативные документами в области технической защиты информации; - угрозы информационной безопасности объекта информатизации; - методы и средства технической защиты информации. Уметь: - проектировать систему защиты с использование программно-аппаратных средств защиты информации; - формировать и анализировать показатели защищенности; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - составлять план управления рисками; - классифицировать функциональность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых систем; - настраивать основные типы телекоммуникационного оборудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные криптографические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты ин-

				формации; - определять необходимые принципы организации защиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области технической защиты информации; - определить опасные угрозы информационной безопасности объекта информатизации; - определить необходимые методы и средства технической защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного оборудования IP сетей; - основными пакетами, применяемыми для расчётов и моделирования в телекоммуникациях; - практическими навыками применения современных криптографических алгоритмов и протоколов; - практическими навыками работы с известными криптографическими библиотеками; - практическими навыками применения национальных стандартов Российской Федерации в области криптографической защиты информации при разработке ПО в области информационной безопасности; - практическими навыками тестирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - практическими навыками организации защиты информации от утечки по техническим каналам на объектах информатизации; - практическими навыками применения нормативных до-

				кументов в области технической защиты информации; - практическими навыками анализа и оценки угроз информационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации.
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.4 ОПК-10.5 ОПК-10.6 ОПК-10.9 ОПК-10.10 ОПК-10.14 ОПК-10.15 ОПК-10.16 ОПК-10.17 ОПК-10.18 ОПК-10.19 ОПК-10.20 ОПК-10.25 ОПК-10.26 ОПК-10.27 ОПК-10.28	Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами. Умеет применять математические методы при исследовании криптографических алгоритмов. Владеет навыками использования типовых криптографических алгоритмов. Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач. Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях. Умеет исследовать и решать сравнения в кольцах вычетов. Умеет использовать достаточные условия простоты для построения больших простых чисел. Умеет оценивать теоретическую сложность применяемых алгоритмов. Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов. Владеет методами построения быстрых вычислительных алгоритмов алгебры и теории чисел. Умеет разворачивать	Знать: - принципы построения сетей связи и передачи информации; - принципы взаимодействия телекоммуникационных систем согласно принципам взаимодействия открытых систем; - основные тренды развития телекоммуникаций; - математические основы симметричных и асимметричных криптографических систем; - принципы работы симметричных и асимметричных криптографических систем, принципы генерации, хранения и использования криптографических ключей, принципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, современные стандарты шифрования, хеширования, электронной подписи; - основные принципы классификации и количественных характеристик технических каналов утечки информации; - основные способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - основы принципов организации защиты информации от утечки по техническим каналам на объектах информатизации; - основные нормативные документами в области технической защиты информации; - угрозы информационной безопасности объекта информатизации; - методы и средства технической защиты информации. Уметь: - классифицировать функциональность элементов сетей связи и передачи информации

			инфраструктуру открытых ключей для решения криптографических задач. Умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность). Умеет решать типовые задачи кодирования и декодирования. Владеет основами построения математических моделей текстовой информации и моделей систем передачи информации. Владеет навыками применения математического аппарата для решения прикладных теоретико-информационных задач.	по семиуровневой модели взаимодействия открытых систем; - настраивать основные типы телекоммуникационного оборудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные криптографические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - определять необходимые принципы организации защиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области технической защиты информации; - определить опасные угрозы информационной безопасности объекта информатизации; - определить необходимые методы и средства технической защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного оборудования IP сетей; - основными пакетами, применяемыми для расчётов и моделирования в телекоммуникациях; - практическими навыками применения современных криптографических алгоритмов и протоколов; - практическими навыками работы с известными криптографическими библиотеками; - практическими навыками применения национальных стандартов Российской Федерации в области криптографической защиты информации при разработке ПО в об-

				ласти информационной безопасности; - практическими навыками тестирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - практическими навыками организации защиты информации от утечки по техническим каналам на объектах информатизации; - практическими навыками применения нормативных документов в области технической защиты информации; - практическими навыками анализа и оценки угроз информационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации.
ОПК-1.1	Способен проводить анализ защищенности и находить уязвимости компьютерной системы	ОПК-1.1.1 ОПК-1.1.2 ОПК-1.1.3 ОПК-1.1.4 ОПК-1.1.5 ОПК-1.1.6 ОПК-1.1.7	Знает принципы построения защищенных компьютерных систем и сетей. Знает требования основных стандартов по оценке защищенности компьютерных систем и сетей. Умеет определять уровень защищенности и доверия программно-аппаратных средств защиты информации. Умеет классифицировать информационные системы по требованиям защиты информации. Умеет определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе. Умеет выполнять анализ компьютерной системы с целью определения уровня защи-	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требований и оценки защищенности систем обработки информации; порядок сертификации защищенных систем обработки информации; - источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей информационных систем, методы оценки рисков информационных систем, методы и средства проектирования технологически безопасного программного обеспечения; - источники угроз информационной безопасности в компьютерных системах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамического анализа кода, методы устранения уязвимостей;

			щенности и доверия. Умеет проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей.	- известные методы анализа ПО на наличие уязвимостей, методы статического и динамического анализа программ, методы проведения экспертизы исходного кода; - принципы функционирования программных средств криптографической защиты информации. Уметь: - определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования; - составлять задание по безопасности и профиль защиты при создании защищенных систем обработки информации; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полученные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззингтестирование); - применять на практике полученные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - практическими навыками применения стандартов информационной безопасности при создании защищенных систем обработки информации; - навыками использования инструментальных интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации; - практическими навыками использования инструментальных средств для модели-

				рования угроз безопасности в компьютерных системах с учетом мер по их предотвращению и проектирования технологически безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования специализированных утилит статического и динамического анализа кода; - специализированными инструментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алгоритмы.
ОПК-11	Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	ОПК-11.4 ОПК-11.5 ОПК-11.9 ОПК-11.10	Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем. Умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками. Умеет формулировать и настраивать политику безопасности основных операционных систем. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.	Знать: - принципы формирования политик безопасности для компьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации информационных систем в соответствии с требованиями по защите информации. Уметь: - проектировать систему защиты с использование программно-аппаратных средств защиты информации; - формировать и анализировать показатели защищенности; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - составлять план управления рисками. Владеть: - навыками контроля комплекса мер безопасности информации на защищаемом объекте с учетом требований руководящих и нормативных документов.

ОПК-1.2	Способен оценивать корректность программных реализаций алгоритмов защиты информации	ОПК-1.2.1 ОПК-1.2.2 ОПК-1.2.3 ОПК-1.2.4 ОПК-1.2.5 ОПК-1.2.6	Знает основные средства и методы защиты программного обеспечения от анализа и нарушения целостности. Знает теоретические основы устранения избыточности данных. Знает основные алгоритмы кодирования данных и сжатия текстовой, графической, аудио- и видеоинформации. Умеет проводить анализ программ и алгоритмов сжатия данных на предмет соответствия требованиям защиты информации. Умеет применять средства и методы анализа программных реализаций для поиска уязвимостей. Знает основные типы уязвимостей программного обеспечения.	Знать: - основные понятия и методы дискретной математики, которые используются для построения моделей и конструирования алгоритмов; - основные понятия, принципы и подходы к кодированию, передаче и обработке информации; - основные численные методы решения математических задач, методы оценки и контроля погрешностей; - источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей информационных систем, методы оценки рисков информационных систем, методы и средства проектирования технологически безопасного программного обеспечения; - источники угроз информационной безопасности в компьютерных системах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамического анализа кода, методы устранения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и динамического анализа программ, методы проведения экспертизы исходного кода; - принципы функционирования программных средств криптографической защиты информации. Уметь: - реализовывать методы дискретной математики на ЭВМ; - переводить числа между различными системами счисления; - рассчитывать степень избыточности кода и оценивать возможности его сжатия; - реализовывать численные методы на ЭВМ; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полученные знания и навыки для

				проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззингтестирование); - применять на практике полученные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - методами построения префиксных кодов для оптимального кодирования данных; - навыками квалифицированного выбора и адаптации существующих методов приближенного решения математических задач, разработки прикладных программ; - навыками использования инструментальных интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации; - практическими навыками использования инструментальных средств для моделирования угроз безопасности в компьютерных системах с учетом мер по их предотвращению и проектирования технологически безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования специализированных утилит статического и динамического анализа кода; - специализированными инструментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алгоритмы.
ОПК-12	Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12.4 ОПК-12.5 ОПК-12.7	Владеет навыками системного программирования. Умеет осуществлять администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отече-	Знать: - архитектуру и принципы построения и защиты операционных систем; - программные интерфейсы настроек политик управления доступом в операционных системах UNIX, FreeBSD, GNU/Linux и MS Windows; - стандартные средства и ме-

			ственного производства. Умеет восстанавливать работоспособность программ специального назначения при возникновении нештатных ситуаций.	тоды восстановления состояний операционных и файловых систем. Уметь: - использовать встроенные средства защиты информации операционных систем GNU/Linux и MS Windows для противодействия угрозам безопасности информации; - использовать встроенные и сторонние средства восстановления информации. Владеть: - навыками настройки антивирусной защиты и сетевого экрана операционных систем GNU/Linux и MS Windows; - создания точек восстановления операционных систем; - навыками работы с программным обеспечением для восстановления файловой системы.
ОПК-1.3	Способен проводить тестирование и использовать средства верификации механизмов защиты информации	ОПК-1.3.1 ОПК-1.3.2 ОПК-1.3.3	Знает основные способы и средства верификации программ. Знает основные способы тестирования средств защиты информации с использованием средств верификации программ. Умеет применять основные методы верификации программ и алгоритмов на предмет соответствия требованиям защиты информации.	Знать: - источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей информационных систем, методы оценки рисков информационных систем, методы и средства проектирования технологически безопасного программного обеспечения; - источники угроз информационной безопасности в компьютерных системах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамического анализа кода, методы устранения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и динамического анализа программ, методы проведения экспертизы исходного кода Уметь: - применять на практике полученные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззингтестирование); - применять на практике полученные знания и навыки для

				анализа ПО на наличие уязвимостей. Владеть: - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования специализированных утилит статического и динамического анализа кода; - специализированными инструментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алгоритмы.
ОПК-13	Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.1 ОПК-13.2 ОПК-13.5 ОПК-13.6 ОПК-13.7 ОПК-13.12 ОПК-13.13 ОПК-13.14 ОПК-13.15 ОПК-13.16 ОПК-13.17 ОПК-13.18 ОПК-13.19 ОПК-13.21 ОПК-13.23 ОПК-13.24	Умеет формулировать и настраивать политику безопасности основных операционных систем. Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств. Умеет работать с интегрированными средами разработки программного обеспечения. Владеет навыками разработки, отладки, документирования и тестирования программ. Владеет навыками использования инструментальных средств отладки и дизассемблирования программного кода. Умеет формализовать поставленную задачу. Умеет разрабатывать эффективные алгоритмы и программы. Умеет проводить оценку вычислительной сложности алгоритма. Умеет планировать разработку сложного программного обеспечения. Владеет методами оценки качества гото-	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского процессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительности ЭВМ; - классификацию современных компьютерных систем и архитектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности применения языков программирования высокого уровня; - язык программирования высокого уровня, структурное и объектно-ориентированное программирование. - способы построения и применения логических выражений в реализации условных операторов и циклов; - технологии построения алгоритмов для решения практических задач;

			вого программного обеспечения. Владеет навыками разработки алгоритмов для решения типовых профессиональных задач. Умеет применять средства и методы анализа программного обеспечения для выявления закладок. Умеет применять методы анализа проектных решений для обеспечения защищенности компьютерных систем. Уметь применять современные средства обеспечения информационной безопасности программ и данных. Умеет проводить анализ программных средств, применяемых для контроля и защиты информации. Умеет проводить аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.	- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинаторных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программного кода; - правила математической логики, для составления логических выражений в алгоритмах программ; - состав и принципы функционирования программно-аппаратных средств защиты информации; - принципы формирования политики информационной безопасности организации; - источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей информационных систем, методы оценки рисков информационных систем, методы и средства проектирования технологически безопасного программного обеспечения; - источники угроз информационной безопасности в компьютерных системах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамического анализа кода, методы устранения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и динамического анализа программ, методы проведения экспертизы исходного кода; - принципы функционирования программных средств криптографической защиты

				информации. Уметь: - объяснять основополагающие принципы создания и развития архитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию технических компьютерных средств, требующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать программно-аппаратные средства защиты информации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построения защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования; - составлять задание по безопасности и профиль защиты при создании защищенных систем обработки информации; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование

				угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полученные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззингтестирование); - применять на практике полученные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной работы с компьютером, программирования на машинно-ориентированном языке; - базовой подготовкой в области программирования для решения практических задач в области информационных систем и технологий; - навыками разработки программ; - навыками разработки, документирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и отладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требований; - практическими навыками применения стандартов информационной безопасности при создании защищенных систем обработки информации; - навыками использования инструментальных интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации; - практическими навыками использования инструментальных средств для моделирования угроз безопасности в компьютерных системах с учетом мер по их предотвращению и проектирования технологически безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо-

				стей, навыками использования специализированных утилит статического и динамического анализа кода; - специализированными инструментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алгоритмы.
ОПК-14	Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации	ОПК-14.4 ОПК-14.5 ОПК-14.6 ОПК-14.11 ОПК-14.12 ОПК-14.13 ОПК-14.14	Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных. Умеет настраивать и применять современные системы управления базами данных. Владеет методикой и навыками составления запросов для поиска информации в базах данных. Умеет пользоваться средствами защиты, предоставляемыми СУБД. Умеет создавать дополнительные средства защиты баз данных. Умеет проводить анализ и оценивание механизмов защиты баз данных. Владеет методикой и навыками использования средств защиты, предоставляемых СУБД.	Знать: - понятие защищенной системы баз данных, этапы и методы проектирования защищенных систем баз данных, модели представления информации на концептуальном, логическом и физическом уровнях, нормальные формы баз данных и алгоритмы их построения, критерии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компьютерных систем, методы обеспечения конфиденциальности, целостности и доступности в системах баз данных, возможности языка SQL (TransactSQL) при обеспечении целостности и конфиденциальности информации в системах баз данных; - этапы и методы проектирования защищенных систем с базами данных, методы обеспечения конфиденциальности, целостности и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической логики, для составления логических выражений в алгоритмах программ. Уметь: - разрабатывать функциональную и информационную модели защищенной системы баз данных, включая концептуальную, логическую и физическую модели; разрабатывать нормализованную схему базы данных; - применять методы защиты информации в системах

				управления базами данных; - осуществлять проектирование и реализацию защищенных систем баз данных с использованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, построения нормализованных баз данных, навыками разработки функциональной и информационной моделей системы баз данных с использованием инструментальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения целостности и конфиденциальности СУБД; - навыками работы с инструментальными средствами проектирования баз данных, системами управления базами данных, средствами обеспечения целостности и конфиденциальности СУБД.
ОПК-15	Способен администрировать компьютерные сети и контролировать корректность их функционирования	ОПК-15.5 ОПК-15.6 ОПК-15.7 ОПК-15.8	Умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах. Умеет осуществлять проектирование и оптимизацию функционирования компьютерных сетей. Владеет навыками администрирования компьютерных сетей. Владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением.	Знать: - полномочную и дискреционную политики доступом; - архитектуру, функции и способы внедрения в инфраструктуру криптографической защиты информации. Уметь: - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами выбора типов и топологий сетевого экранирования; - навыками развертывания и настройки программно-аппаратных средств защиты информации.
ОПК-16	Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	ОПК-16.6 ОПК-16.7 ОПК-16.8 ОПК-16.9 ОПК-16.10 ОПК-16.12 ОПК-16.14 ОПК-16.16	Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения	Знать: - принципы построения сетей связи и передачи информации; - принципы взаимодействия телекоммуникационных систем согласно принципам взаимодействия открытых систем; - основные принципы классификации и количественных характеристик технических

			вторжений для защиты информации в сетях. Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Владеет навыками настройки межсетевых экранов. Владеет методиками анализа сетевого трафика. Умеет выявлять действие вредоносных программ, и определять характер их воздействия. Умеет производить оценку технического состояния аппаратных средств защиты информации. Умеет выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.	каналов утечки информации; - основные способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - основы принципов организации защиты информации от утечки по техническим каналам на объектах информатизации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства технической защиты информации. Уметь: - классифицировать функциональность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых систем; - настраивать основные типы телекоммуникационного оборудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные криптографические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - планировать и устанавливать инфраструктуры открытых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного оборудования IP сетей; - основными пакетами, применяемыми для расчётов и моделирования в телекоммуникациях; - практическими навыками применения современных криптографических алгоритмов и протоколов; - практическими навыками работы с известными крипто-

				графическими библиотеками; - методами обеспечения защиты данных на этапе передачи в IP-сетях; - методами выбора типов и топологий сетевого экранирования; - навыками развертывания и настройки программно-аппаратных средств защиты информации.

13. Объем практики в зачетных единицах / ак. час. — 6/216.
Форма промежуточной аттестации - *зачет с оценкой*.

14. Виды учебной работы

Вид учебной работы	Трудоемкость					
	Всего	По семестрам				
		№ 10		№ семестра		
		ч.	ч., в форме ПП	ч.	ч., в форме ПП	…
Всего часов	216	216	216			
в том числе:						
Лекционные занятия (контактная работа)						
Практические занятия (контактная работа)	3	3	3			
Самостоятельная работа	213	213	213			
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*						
Итого:	216	216	216			

15. Содержание практики (или НИР)

№ п/п	Разделы (этапы) практики	Содержание раздела
1	Подготовительный	Инструктаж по технике безопасности, общее знакомство с местом практики (научно-исследовательскими лабораториями), составление и утверждение графика прохождения практики, изучение литературных источников по теме экспериментального исследования, реферирование научного материала и т.д.
2	Основной (экспериментальный, исследовательский и т.д.)	Освоение методов исследования, выполнение производственных заданий, проведение самостоятельных экспериментальных исследований, посещение отделов предприятий, знакомство с особенностями организационно-управленческой деятельности предприятия и т.д.
3	Заключительный (информационно-аналитический)	Обработка экспериментальных данных, составление и оформление отчета и т.д.

16. Перечень учебной литературы, ресурсов сети «Интернет», необходимых для прохождения практики

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Казарин Олег Викторович. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов : [для студ. вузов, обучающихся по инженер.-техн. направлениям] / О.В. Казарин, А.С. Забабурин .— Москва : Юрайт, 2018 .— 311, [1] с. : ил., табл. — (Специалист) .— Библиогр. в конце гл. — ISBN 978-5-9916-9043-0.
2	Баранова Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330 .— ISBN 978-5-369-01761-6.

3	Мельников Владимир Павлович. Информационная безопасность : [учебник для студ. вузов, обучающихся по направлениям подготовки "Конструкторско-технологическое обеспечение машиностроительных производств", "Автоматизация технологических процессов и производств"] / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева; под ред. В.П. Мельникова.—2-е изд.,перераб. и доп.—Москва: КноРус, 2018 .—371 с.:ил.,цв.ил.,табл.—(Бакалавриат) .— Библиогр.: с. 369-371
4	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351
5	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
6	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с. <URL:http://www.methodolog.ru/books/mni.pdf>
7	Митрофанова Е.Ю., Сирота А.А. Методические указания по оформлению выпускных работ бакалавров / Е.Ю., Митрофанова, А.А. Сирота, учебно-методическое пособие, - Воронеж: Издательский дом ВГУ, 2016 – 23 с.
8	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
9	Фостер, Джеймс. Защита от взлома: сокеты, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 р. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
10	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите : / Э. Скудис .— Москва : ДМК Пресс, 2009 .— 512 с. : ил. — (Защита и администрирование) .— .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.
11	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виега ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
12	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.
13	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) . Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.

б) дополнительная литература:

№ п/п	Источник
14	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва : Флинта : Наука, 2014. — 108 с.
15	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. – Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269.
16	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва : Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348.
17	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
18	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
19	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)
20	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).

21	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
22	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
23	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.
24	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб. : БХВ-Петербург, 2006. - 464 с.
25	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
26	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII международ. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
27	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
28	Андрианов В. И. "Шпионские штучки 2", или Как сберечь свои секреты / Под общ. ред. Колесниченко О. В. и др. — СПб. : Полигон, 1997 .— 271 с. — ISBN 5-89173-015-4 : 12.33.
29	Брусницин Н.А. Открытость и шпионаж / Н.А.Брусницин. – М.: Воениздат, 1991.
30	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
31	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
32	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
33	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет) *:

№ п/п	Ресурс
34	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
35	Фундаментальные и прикладные исследования в области параллельных вычислений [электр. ресурс]. – Режим доступа http://parallel.ru/research свободный.
36	Элементы теории чисел и криптозащита : учебное пособие для вузов. Ч. 2 / Воронеж. гос. ун-т; сост.: Б.Н. Воронков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 95 с. : ил. — Библиогр.: с.95 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-238.pdf>
37	http://www.cryptopro.ru
38	http://www.infotecs.ru
39	http://www.rsdn.ru/article/crypto/cspsecrets.xml Секреты разработки CSP для Windows. Создание криптографического провайдера для Windows. Зырянов Юрий Сергеевич, ООО “ЛИССИ”. Источник: RSDN Magazine #3-2006
40	http://www.lissi-crypto.ru/
41	http://www.signal-com.ru
42	http://www.shipka.ru
43	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
44	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/).
45	«Университетская библиотека online» - Контракт № 3010-07/33-19 от 11.11.2019 «Консультант студента» - Контракт № 3010-07/34-19 от 11.11.2019 ЭБС «Лань» - Договор 3010-04/05-20 от 26.02.2020. «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018 ЭБС «Юрайт» - Договор № 43/8 от 10.02.2020.

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

17. Информационные технологии, используемые при проведении практики, включая программное обеспечение и информационно-справочные системы (при необходимости)

Практика проводится на профильных предприятиях (организациях, учреждениях, фирмах), с которыми заключены договора на прохождение практики, а также в аудиториях, компьютерных и специализированных лабораториях факультета компьютерных наук ВГУ. Предприятия предоставляют студентам материально-техническую базу для прохождения практики.

18. Материально-техническое обеспечение практики:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Практика проводится на профильных предприятиях (организациях, учреждениях, фирмах), с которыми заключены договора на прохождение практики, а также в аудиториях, компьютерных и специализированных лабораториях факультета компьютерных наук ВГУ. Предприятия предоставляют студентам материально-техническую базу для прохождения практики.

N п/п	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	Учебная аудитория: персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 19" (30 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 316П
2	Лаборатория информационной безопасности компьютерных систем: персональные компьюте-ры на базе i3-8100-3,9ГГц, мониторы ЖК 24" (13 шт.), мультимедийный проектор, экран. Лабораторное оборудование программно-аппаратных средств обеспечения информацион-ной безопасности: персональные компьютеры на базе Intel i3-8100 3.60ГГц, мониторы ЖК 19" (10 шт.), стойка (коммуникационный шкаф), управля-емый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лаборатор-ная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528. Учебно-методический комплекс "Программно-аппаратная защита сетей с защитой от НСД" ОАО "ИнфоТеКС".	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 303П
3	В соответствии с договором № 427 от 20.05.2019 о практической подготовке обучающихся	107023, г. Москва, ул. Измайловский Вал, д. 30, ООО «Философия.ИТ» (Лига цифровой экономики)
4	В соответствии с договором № 564 от 11.05.2021 о практической подготовке обучающихся	394036, г. Воронеж, ул. Карла Маркса, д. 53, оф. 501, ООО «Ангелы ИТ
5	В соответствии с договором № 273 от 24.02.2021 о практической подготовке обучающихся	125009, г. Москва, ул. Воздвиженка, д. 10, Акционерное общество «Банк ДОМ.РФ»
6	В соответствии с договором № 22/01-2 от 20.01.2022 о практической подготовке обуча-	394018, г. Воронеж, ул. Свободы, д. 69, оф. 45, ООО «ЭЛ-ЭКС»

	ющихся	
7	В соответствии с договором №22/02-10 от 21.02.2022 о практической подготовке обучающихся	394006, г. Воронеж, ул. Карла Маркса, д. 46 Управление Федеральной налоговой службы по Воронежской области
8	В соответствии с договором № 1431 от 19.07.2019 г. о практической подготовке обучающихся	394036, г. Воронеж, ул. Карла Маркса, д. 70 Департамент финансов Воронежской области
9	В соответствии с договором № 22/05-20 от 05.05.2022 о практической подготовке обучающихся	394018, г. Воронеж, ул. Средне-Московская, д. 1Д, пом. 1, ООО «СёрфСтудио»
10	В соответствии с договором № 22/03-100 от 30.03.2022 о практической подготовке обучающихся	443090, Самарская область, г. Самара, улица Гастелло, дом 43А, помещение Н15, ООО «Хоулмонт Самара»
11	В соответствии с договором № 22/01-1 от 20.01.2022 о практической подготовке обучающихся	394026, г. Воронеж, ул. Текстильщиков, д. 5Б, пом. 177, ООО «ФИТТИН»
12	В соответствии с договором № 35-22-01/09600/355 от 31.03.2022 - № 22/04-44 зарег. 12.04.2022 о практической подготовке обучающихся	196084, г. Санкт-Петербург, ул. Киевская, д. 5, к. 4 ООО «Газпромнефть-Цифровые решения»
13	В соответствии с договором № 22/05-21 от 05.05.2022 г. о практической подготовке обучающихся	394000, г. Воронеж, ул. Пятницкого, 55 ООО ТК «Контакт»
14	В соответствии с договором № 22/05-36 от 12.05.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Средне-Московская, д. 6а, помещение V ООО «Техномаркет
15	В соответствии с договором № ДОГ-3500-22-000000176 – 22/06-28 от 27.05.2022 г. зарег. 06.06.2022 г. о практической подготовке обучающихся	162602, Вологодская обл., г. Череповец, ул. Ленина, д. 123А ОАО «Северсталь — Инфоком»

19. Оценочные средства для проведения текущей и промежуточной аттестации обучающихся по практике

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Раздел (этап) Подготовительный	ОПК-5 ОПК-9 ОПК-10 ОПК-1.1 ОПК-11 ОПК-13 ОПК-14	Способен: - применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; - решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности; - проводить анализ защищенности и находить уязвимости компьютерной системы; - разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации; - разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и прово-	Дневник практики, Отчет по практике.

			дить анализ их безопасности; - проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации.	
2.	Раздел (этап) экспериментальный, исследовательский	ОПК-6 ОПК-10 ОПК-11 ОПК-12 ОПК-1.3 ОПК-13 ОПК-14 ОПК-15 ОПК-16	Способен: - при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; - анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности; - разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации; - администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения; - проводить тестирование и использовать средства верификации механизмов защиты информации; - разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности; - проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации; - администрировать компьютерные сети и контролировать корректность их функционирования; - проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	Дневник практики, Отчет по практике.
3.	Заключительный (информационно-аналитический)	ОПК-1.2 ОПК-1.3 ОПК-15 ОПК-16	Способен: - оценивать корректность программных реализаций алгоритмов защиты информации; - проводить тестирование и использовать средства верификации механизмов защиты информации; - администрировать компьютерные сети и контролировать корректность их функционирования; - проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	Дневник практики, Отчет по практике.

Промежуточная аттестация форма контроля – зачет с оценкой	

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания и критерии их оценивания

20.1 Текущий контроль успеваемости Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Оценка знаний, умений и навыков, характеризующих этапы формирования компетенций, при прохождении практики проводится в ходе промежуточной аттестаций. Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

20.2 Промежуточная аттестация Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

СТРУКТУРА ОТЧЕТА ПО ПРАКТИКЕ

1. Отчет по практике должен включать титульный лист, содержание, введение, описание теоретических и практических аспектов выполненной работы, заключение, необязательный список использованных источников, приложения.
2. На титульном листе должна быть представлена тема практики, группа и фамилия студента, данные о предприятии, на базе которого выполнялась практика, фамилия руководителя.
3. Во введении студенты должны дать краткое описание задачи, решаемой в рамках практики.
4. В основной части отчета студенты приводят подробное описание проделанной теоретической и (или) практической работы, включая описание и обоснование выбранных решений, описание программ и т.д.
5. В заключении дается краткая характеристика проделанной работы, и приводятся ее основные результаты.
6. В приложениях приводятся непосредственные результаты разработки: тексты программ, графики, диаграммы, и т.д.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА

1. Отчет оформляется в печатном виде, на листах формата А4.
2. Основной текст отчета выполняется шрифтом 13-14 пунктов, с интервалом 1,3-1,5 между строками. Текст разбивается на абзацы, каждый из которых включает отступ и выравнивание по ширине.
3. Текст в приложениях может быть выполнен более мелким шрифтом.
4. Отчет разбивается на главы, пункты и подпункты, включающие десятичную нумерацию.
5. Рисунки и таблицы в отчете должны иметь отдельную нумерацию и названия.
6. Весь отчет должен быть оформлен в едином стиле: везде в отчете для заголовков одного уровня, основного текста и подписей должен использоваться одинаковый шрифт.
7.Страницы отчета нумеруются, начиная с титульного листа. Номера страниц проставляются в правом верхнем углу для всего отчета кроме титульного листа.
8. Содержание отчета должно включать перечень всех глав, пунктов и подпунктов, с указанием номера страницы для каждого элемента содержания.
9. Ссылки на литературу и другие использованные источники оформляются в основном тексте, а сами источники перечисляются в списке использованных источников.

Описание технологии проведения

Промежуточная аттестация по практике включает подготовку и защиту отчета/проекта и/или выполнение практического задания.

Отчет содержит следующие составляющие: обработанный и систематизированный материал по тематике практики; экспериментальную часть, включающую основные методы проведения исследования и статистической обработки, обсуждение полученных результатов; заключение, выводы и список литературных источников. Отчет обязательно подписывается (заверяется) руководителем практики. Результаты прохождения практики докладываются обучающимся в виде устного сообщения с демонстрацией презентации на заседании кафедры (заключительной конференции).

По результатам доклада с учетом характеристики руководителя и качества представленных отчетных материалов обучающемуся выставляется соответствующая оценка. Дифференцированный зачет по итогам практики выставляется обучающимся руководителем практики на основании доклада и отчетных материалов, представленных обучающимся.

При оценивании используются количественные шкалы оценок.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Программа практики выполнена в полном объеме и в соответствии с утвержденным графиком. Подготовленные отчетные материалы отражают адекватное формулирование цели и задач исследования, выбранный метод обеспечил решение поставленных в ходе практики задач	Повышенный уровень	Отлично
Программа практики выполнена в соответствии с утвержденным графиком. Подготовленные отчетные материалы и представленный доклад не соответствует одному (двум) из перечисленных критериев. Недостаточно продемонстрировано, или содержатся отдельные пробелы.	Базовый уровень	Хорошо
Обучающийся частично выполнил план работы практики (не менее 50%). В представленных отчетных материалах выявлено несоответствие выбранного метода цели и задачам исследования. При прохождении практики не были выполнены все поставленные перед практикантом задачи (можно привести перечень задач практики), отчетные материалы имеют ряд недочетов по объему, необходимым элементам и качеству представленного материала.	Пороговый уровень	Удовлетворительно
Обучающийся не выполнил план работы практики. В представленных отчетных материалах отсутствуют необходимые элементы: нет отзыва научного руководителя, не сформулированы цель и задачи работы, не приведены или ошибочны предложенные методы и т.д.	–	Неудовлетворительно