МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ»

Уровень подготовки: высшее образование – магистратура

Направление подготовки
10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(код и наименование направления подготовки)

Направленность подготовки
Информационная безопасность
(наименование программы подготовки)

Квалификация (степень) выпускника
магистр

Форма обучения
очная

Разработана в соответствии

с ФГОС ВПО, Приказ МОиН РФ от 28.10.2009, № 497

Актуализирована в соответствии

с ФГОС ВО, Приказ МОиН РФ от 01.12.2016, № 1513

Уфа 2016

Исполнитель: доцент каф. ВТиЗИ		В.Е.Кладов
ст.преподаватель		С.Н.Зарипов
должность	личная подпись	расшифровка подписи
Заведующий кафедрой ВТиЗИ		В.И.Васильев
наименование кафедры	личная подпись	расшифровка подписи

1. Место дисциплины в структуре образовательной программы

Дисциплина «Технология обеспечения информационной безопасности объектов» является обязательной дисциплиной вариативной части ОПОП по направлению подготовки 10.04.01 Информационная безопасность, направленность: «Информационная безопасность».

Рабочая программа составлена в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 090900 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. № 497;

Рабочая программа актуализирована в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1513.

Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Целью освоения дисциплины является формирование у будущих магистров в области информационной безопасности теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач связанных с использованием технологий обеспечения информационной безопасности объектов.

Задачи:

- изучить концепцию сетевого управления на базе SNMP, методы повышения защищенности сетевого управления;
- научить проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты;
- сформировать умение осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;
- выработать навыки администрирования защищенных операционных систем;
- изучить способы атак на программно-коммутируемые сети и методы защиты SDN сетей;
- научить реализовывать защищенные распределенные вычислительные системы на основе современных технологий обеспечения информационной безопасности объектов;
- привить навыками защиты информации в виртуальных средах и облачных платформах.

Дисциплина является самостоятельным элементом в системе подготовки научно-педагогических кадров высшей квалификации. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- теоретические основы компьютерной безопасности;
- управление информационной безопасностью.

В дисциплине «Технология обеспечения информационной безопасности объектов» определяются теоретические основы и практические навыки, при освоении которых магистрант способен приступить к прохождению научно-исследовательской практики и выполнять научные исследования в соответствующей предметной области.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию

1	способность понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности, оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией развития организации	ПК-1	Базовый уровень	Управление информационной безопасностью
2	способностью разработать программы и методики испытаний, организовать тестирование и отладку программно-аппаратных, криптографических и технических систем и средств обеспечения информационной безопасности	ПК-5	Базовый уровень	Теоретические основы компьютерной безопасности
3	способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7	Базовый уровень	Теоретические основы компьютерной безопасности
4	способен организовать работу по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ПК-14	Базовый уровень	Управление информационной безопасностью

- **пороговый уровень дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;*

*-**базовый уровень** позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;*

*-**повышенный уровень** предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.*

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины, практики, научных исследований для которых данная компетенция является входной
1	способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	ОПК-2	Повышенный уровень	Производственная практика
2	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	Повышенный уровень	Производственная практика Преддипломная практика Подготовка магистерской диссертации

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	способность разрабатывать, системы, комплексы, средства и технологии обеспечения информационной безопасности	ПК-2	Концепцию сетевого управления на базе SNMP, методы повышения защищенности сетевого управления	Осуществлять выбор функциональной структуры системы обеспечения информационной безопасности	Навыками администрирования защищенных операционных систем
2	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ПК-4	Способы атак на программно-коммутируемые сети и методы защиты SDN сетей	Реализовывать защищенные распределенные вычислительные системы на основе современных технологий обеспечения информационной безопасности объектов	навыками защиты информации в виртуальных средах и облачных платформах

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетные единицы (180 часов).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.	Трудоемкость, час.

	1 семестр	2 семестр
Лекции (Л)	–	20
Практические занятия (ПЗ)	–	26
Лабораторные работы (ЛР)	–	12
КСР	–	5
Курсовая проект работа (КР)	–	не предусмотрено планом
Расчетно - графическая работа (РГР)	–	не предусмотрено планом
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	–	81
Подготовка и сдача экзамена	–	36
Подготовка и сдача зачета (контроль)	–	–
Вид итогового контроля (зачет, экзамен)	–	экзамен

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
		Аудиторная работа				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1	**Защищенные операционные системы.** Сертифицированные операционные системы на базе windows и Linux. ОС МСВС. Astra-Linux Special Edition. Область применения. Релизы. Компоненты. Реализованные функции защиты от НСД. Ключевые особенности. Семейство «Заря». Основные компоненты, их возможности, особенности, архитектура	2		4	1	6	13	Р 6.1, №1 Р 6.2, №4	*лекция-визуализация, проблемное обучение, обучение на основе опыта, компьютерная симуляция*
2	**Защищенные распределенные вычислительные системы** Архитектура безопасности фирмы Cisco. Высокоуровневое представление архитектуры безопасности. Топология Интернет периметра. Особенности межсетевых экранов следующего поколения. Требования к современным системам обнаружения атак. Мониторинг информационной безопасности на уровне приложений. Топология и защита удаленных офисов. Распределенные сетевые сервисы обеспечения информационной безопасности Cisco Security Intelligence Operation(SIO). Архитектура безопасности Cisco Secure X. Аспекты защиты архитектуры Secure X. Cisco TrustSec и Cisco Identify Services Engine. Решения Cisco по защите мобильного и удаленного доступа. Технология и функции Cisco AnyConnect. Решение Cisco Safe Scan. Решения Cisco по защите облачных вычислений. Решения фирмы Checkpoint по реализации защищенных распределенных вычислительных систем. Продукты фирмы Checkpoint. Шлюзы безопасности. Устройства управления безопасностью. Защита рабочих станций. Аутентификация	7	22	4	2	34	69	Р 6.1, №1 Р 6.2, №5 Р 6.2, №1 Р 6.2, №2 Р 6.2, №3	*лекция-визуализация, проблемное обучение, обучение на основе опыта, компьютерная симуляция*

	и контроль доступа. Особенности реализации VPN сетей. Средства анализа защищенности. Обманные системы.								
3	**Защита информации в виртуальных средах и облачных платформах** Специфика обработки данных в виртуальной среде. Средства управления виртуальной инф-раструктурой. Классификация угроз безопасности в виртуальной среде. Требования ФСТЭК по защите среды виртуализации. Защитные программные продукты для виртуальных сред. Защита от не-санкционированного доступа. Сетевая безопасность виртуальных сред. Системы предотвращения вторжений. Средства резервного копирования для виртуальных сред. Семейство продуктов vGate R2 компании «Код Безопасности» для защиты объектов виртуальных инфраструктур предприятий, функцио-нирующих на основе продуктов компании VMware и на основе платформы Microsoft Hyper-V. Основные возможности, механизмы защиты виртуальных машин. Развертывание и конфигурация основных компонентов защиты VGate. Агент авторизации VGate Client Облачные вычисления Модели обслуживания и развертывания облачных вычислений. Основные характеристики «облачных вычислений. Концепция архитектуры «облачной системы». Безопасность облачных вычислений. Основные проблемы безопасности облачной инфраструктуры Средства защиты в виртуальных средах. Основные понятия Microsoft Azure. Компоненты Azure. Портал управления. Среда выполнения	4	4	4	1	26	39	Р 6.1, №1 Р 6.2, №5 Р 6.2, №2 Р 6.2, №3	*лекция-визуализация, проблемное обучение, обучение на основе опыта, компьютерная симуляция*

	приложений. Виртуальные машины Azure. Веб-приложения. Облачные службы. Управление данными. Виртуальная сеть. Службы разработки. Мобильные приложения. Создание веб-приложений. Безопасность Windows Azure. Устройство Azure с точки зрения потребителей. И с точки зрения внутренних компонентов. Физическая и сетевая безопасность. Безопасность коммуникаций и среды выполнения. Идентификация, контроль доступа. Безопасность данных. Целостность данных, доступность и надежность.								
4	**Защита систем сетевого управления** Системы сетевого управления на базе SNMP. Концепции SNMP-управления. SNMP. Локализация ключей. Алгоритмы аутентификации и шифрования, используемые в USM. Управление доступом на основе представлений	3			1	6	10	Р 6.1, №1 Р 6.2, №1	*лекция-визуализация,*
5	**Понятие программно-коммутируемых сетей**. Архитектура SDN. Протокол OpenFlow управления процессом обработки данных, передающихся по сети передачи данных маршрутизаторами и коммутаторами, реализующий технологию программно-конфигурируемой сети. Виртуализация в SDN. Направления атак на SDN. Атаки на инфраст-руктурный уровень. Атака на уровень управления. Атаки на уровень приложений. Усиление системы защиты SDN. Защита инфраструктурного уровня. Защита уровня управления. Защита уровня приложений	4			1	8	13	Р 6.1, №1 Р 6.2, №1	*лекция-визуализация, проблемное обучение,*

Занятия, проводимые в интерактивной форме, составляют 16,3% от общего количества аудиторных часов по дисциплине .

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1,2	2	Защита информационных процессов в Active Directory	4
3	2	Распределенный межсетевой экран Trust Access	2
4,5	2	Система комплексной защиты информации Infowatch End-point Security	4
6	2	Анализ уязвимостей XSpider	2
7,8	2	Обманная система Security Studio Honeypot Manager	4
9,10	2	Cisco PIX	4
11,12	3	VGate	4
13	1-5	Выступление студентов с докладами по результатам СРС	2

Лабораторные работы

№ Занятия	№ раздела	Тема	Кол-во часов
1	1	Защищенные операционные системы Astra-Linux	4
2	2	Средство анализа защищенности «Сканер-ВС»	4
3	3	Защита в MS Azure	4

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная литература

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : [учебное пособие] / В. Ф. Шаньгин .— Москва : Форум : Инфра-М, 2013.— 415, [1] с. : ил. ; 21 см .— (Профессиональное образование)

6.2Дополнительная литература

1.Основы информационной безопасности [Электронный ресурс] : [учеб. пособие для студ., обуч по спец. в области информационной безопасности] / Е. Б. Белов [и др.] .— Москва : Горячая линия-Телеком, 2011 .— 544 с. : ил. — Библиогр. в конце гл. — Доступ по логину и паролю из сети УГАТУ .— ISBN 5-93517-292-5 .— <URL:http://e.lanbook.com/view/book/5121/page2/>.

2.Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : [учебное пособие для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника»] / В. Ф. Шаньгин .— Москва : ДМК ПРЕСС, 2012 .— 592 с. — Доступ по логину и паролю из сети УГАТУ .— ISBN 978-5-94074-637-9 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3032>.

3.Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] : [учебное пособие для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника»] / В. Ф. Шаньгин .— Москва : ДМК ПРЕСС, 2010 .— 544 с. — Доступ по логину и паролю из сети УГАТУ .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.

4. Гришина, Н. В. Комплексная система защиты информации на предприятии : [учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов

информации"] / Н. В. Гришина .— Москва : ФОРУМ, 2011 или 2014.— 238 с. : ил. ; 22 см .— (Профессиональное образование)
5. **Сердюк, В. А.** Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В. А. Сердюк ; Государственный университет, Высшая школа экономики .— Москва : Издательский дом Государственного университета- Высшей школы экономики, 2011 .— 572 с. ; 21 см .— ISBN 978-5-7598-0698-1

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Обучающимся обеспечен доступом к электронным ресурсам и информационным справочным системам, перечисленным в таблице

Таблица

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателями
1.	ЭБС «Лань» http://e.lanbook.com/	41716	С любого компьютера, имеющего выход в Интернет, после регистрации в ЭБС по сети УГАТУ	Договор № ЕД – 1185/0208-16 от 08.08.2016
2.	ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru	1225	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Учредительный договор Ассоциации образовательных организаций «Электронное образование Республики Башкортостан» от 29.11.2013
3.	Консорциум аэрокосмических вузов России http://elsau.ru/	1235	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Договор о сетевом взаимодействии от 15.12.2014
4.	Электронная коллекция образовательных ресурсов УГАТУhttp://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus	528	С любого компьютера по сети УГАТУ	Свидетельство о регистрац. №2012620618 от 22.06.2012
5.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	885 898 экз.	Доступ с компьютеров читальных залов	Договор №2255/0208-15 от 23.12.2015

			библиотеки, подключенных к ресурсу	
6.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн. диссертаций и дипломных работ	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и Государственной публичной научно-технической библиотекой России (далее ГПНТБ России) Сублиц. договор №ProQuest/15152/0208-16 от 02.06.2016
7.	СПС «КонсультантПлюс»	2007691 экз.	По сети УГАТУ	Договор 3К-2318/0106-15 от 30.12.2015
8.	СПС «Гарант»	6139026 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор 15\0208-16 от 15.03.2016
9.	ИПС «Технорма/Документ»	36939 экз.	Локальная установка: библиотека УГАТУ-5 мест; кафедра стандартизации и метрологии-1место; кафедра начертательной геометрии и черчения-1 место	Договор № АОСС/914-15 № 989/0208-15 от 08.06.2015.
10.	Научная электронная библиотека eLIBRARY* http://elibrary.ru/	9919 полнотекстовых журналов	С любого компьютера, имеющего выход в Интернет, после регистрации в НЭБ на площадке библиотеки УГАТУ	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА». № 07-06/06 от 18.05.2006
11.	Патентная база данных компании Questel Orbit* http://www.orbit.com	55 млн. документов	С любого компьютера по сети УГАТУ, имеющего выход в	В рамках Государственного контракта от 17.02.2016 г.

			Интернет	№14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор№Questel/15 146/0208-16 от 02.06.2016
12.	Научные полнотекстовые журналы издательства Taylor& Francis Group* http://www.tandfonline.com/	1700 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №T&F/151 44/0208-16 от 02.06.2016
13.	Научные полнотекстовые журналы издательства Sage Publications* http://online.sagepub.com/	790 наимен. жрнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/151 47/0208-16 от 02.06.2016
14.	Научные полнотекстовые журналы издательства Oxford University Press* http://www.oxfordjournals.org/	255 наимен. Журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OUP-151 43/0208-16 от 02.06.2016
15.	База данных Computers & Applied Sciences Complete	1000 наим. журн.	С любого компьютера по	В рамках Государственного

	компании EBSCO Publishing http://search.ebscohost.com		сети УГАТУ, имеющего выход в Интернет	контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №CASC/151 50/0208-16 от 02.06.2016
16.	Научный полнотекстовый журнал Science The American Association for the Advancement of Science http://www.sciencemag.org	1 наимен. журнала.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Science/151 45/0208-16 от 02.06.2016
17.	Научные полнотекстовые журналы Американского института физики http://scitation.aip.org/	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №AIP/151 48/0208-16 от 02.06.2016
18.	Научные полнотекстовые ресурсы Optical Society of America* http://www.opticsinfobase.org/	19 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OSA/151 49/0208-16 от 02.06.2016
19.	База данных GreenFile	5800	С любого	Доступ

	компании EBSCO* http://www.greeninfoonline.com	библиографич записей, частично с полными текстами	компьютера по сети УГАТУ, имеющего выход в Интернет	предоставлен компанией EBSCO российским организациям-участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)
20.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиографич записей		В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор №INSPEC/151 51/0208-16 от 02.06.2016
21.	Архив научных полнотекстовых журналов зарубежных издательств*- http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849– 1995) SAGE Publications (1800-1998) цифровой архив журнала Science (1880 -1996) Taylor & Francis (1798-1997) Институт физики Великобритании The Institute of Physics (1874-2000)	2361 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен российским организациям-участникам консорциума НЭИКОН (в т. ч. УГАТУ - без подписания лицензионного договора)

* Периодические издания получены по Гранту и на баланс библиотеки не принимались.

7 Образовательные технологии

Для достижения наиболее эффективных результатов освоения дисциплины при реализации различных видов учебной работы применяются информационные технологии (использование компьютерных тестирующих средств оценки уровня знаний обучаемых, использование мультимедийного сопровождения лекций, электронных мультимедийных учебных пособий и др.) и интерактивные методы и технологии обучения (проблемные лекции, лекции-

визуализации, технология проблемного обучения, технология развития критического мышления, групповая работа), с учетом содержания дисциплины и видов занятий, предусмотренных учебным планом.

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
2	Л	Лекция-визуализация	6
	ПР	Кейс задачи	4
Итого:			10

Формы работы студентов: лекционные занятия, лабораторные работы, практические занятия, решение кейс-задач, выступление с докладами, решение тестов, ответы на контрольные вопросы.

Дисциплина разбита на модули, представляющие собой логически завершенные части курса и являющиеся теми комплексами знаний и умений, которые подлежат контролю.

Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

В качестве организованной самостоятельной работы студента рекомендуется выступление с докладами по выбранной заранее тематике. При подготовке доклада студент должен в соответствии с требованиями к оформлению сформулировать проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения заданной проблемы.

Для успешной подготовки к итоговому контролю необходимо выполнить следующие контрольные мероприятия:

1. Выполнить лабораторные работы по всем темам дисциплины. Выполнение лабораторных работ требует заполнения отчетов, которые составляются в электронном виде. Файлы отчета с материалами выполненных заданий лабораторных работ должны быть представлены преподавателю. В отчетах должна быть представлена следующая информация: тема работы; цель работы; общая постановка задачи; индивидуальные данные для выполнения работы (№ варианта); результаты выполнения работы; ответы на контрольные вопросы.

2. Выполнены все кейс-задачи. Решение кейс-задач требует представления отчетов, которые составляются в электронном виде. Файлы отчета с материалами выполненных заданий должны быть представлены преподавателю. В отчетах должна быть представлена следующая информация: тема работы; цель работы; общая постановка задачи; индивидуальные данные для выполнения задачи (№ варианта); результаты выполнения каждого пункта задачи; ответы на контрольные вопросы и тесты.

3. Пройти промежуточное тестирование по окончанию освоения очередного модуля учебной дисциплины.

Экзамен проводится аудиторно по экзаменационным билетам. Экзаменационные билеты содержат три вопроса.

9. Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации – 5-301, 5-314.

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

- 5-220 – лаборатория защиты информации;

Вычислительное и телекоммуникационное оборудование, необходимое для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

Компьютеры с процессором не хуже Intel i5, ОЗУ – не менее 2 Гб, винчестер 500.Гб, сетевой картой со скоростью передачи данных 1 Гб/сек

Программное обеспечение, необходимое для реализации ОПОП ВО:

- программный комплекс – операционная система Microsoft Windows (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования);
- программный комплекс – Microsoft Office (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования);
- программный комплекс – операционная система Microsoft Visio Pro (№ договора ЭА-269/0503-16 , 50 компьютеров, на которые распространяется право пользования);
- Kaspersky Endpoint Security для бизнеса (лицензии 1055/0503-16, 500 users);
- контур информационной безопасности SearchInform (UEI-2349-87, 25 пользователей);
- операционная система Astra-Linux Special Edition (договор с АО «НПО РусБИТех» РБТ-14/1318-01-ВУЗ);
- средство анализа защищенности Сканер-ВС (версия для учебных заведений, freeware);
- обманная система Security Studio Honeypot Manager (договор о сотрудничестве с ООО «Код безопасности»);
- vGate(договор о сотрудничестве с ООО «Код безопасности»)
- распределенный межсетевой экран Trust Access (договор о сотрудничестве с ООО «Код безопасности»);
- Infotecs ViPNeT (пробная версия);
- система комплексной защиты информации Infowatch Endpoint Security ; (IWES-S3-DE, 25пользователей).

10. Адаптация рабочей программы для лиц с ОВЗ

При обучении инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, обеспечивается возможность беспрепятственного доступа в учебные помещения и пункты питания и другие, необходимые для жизнедеятельности помещения, оборудованные пандусами, лифтами и иными средствами, облегчающими процесс передвижения. Для лиц с ограниченными возможностями здоровья по зрению предусматривается возможность доступа к зданию с собакой-поводырем.

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.