МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ»

Уровень подготовки: высшее образование – подготовка бакалавров

Направление подготовки бакалавров
09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Направленность подготовки (профиль, специализация)
ЭВМ, системы, сети
(наименование профиля подготовки, специализации)

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Исполнитель: _____*доц., к.т.н.* *Кладов В.Е.*_____
Должность *Фамилия И. О.*

Заведующий кафедрой: _____ *Васильев В.И.*_____
Фамилия И.О.

Уфа 2016

1.Место дисциплины в структуре образовательной программы

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 09.03.01 «*Информатика и вычислительная техника*», утвержденного приказом Министерства образования и науки Российской Федерации от «12» января 2016 г. № 5.

Согласно ФГОС ВО дисциплина «Проектирование защищенных компьютерных систем» является дисциплиной по выбору вариативной части основной профессиональной образовательной программы (ОПОП) по направлению подготовки бакалавра *09.03.01 «Информатика и вычислительная техника», направленность подготовки «ЭВМ. системы, сети».*

Целью освоения дисциплины является формирование у будущих бакалавров формирование систематизированных знаний о роли защиты информационных процессах в компьютерных системах и сетях, об основных моделях угроз информационной безопасности, принципах, методах и направлениях защиты информации в компьютерных системах и сетях.

Задачи:

- сформировать знания о назначении, составе и принципах работы средств защиты информации в компьютерных системах и сетях;
- изучить основные технические характеристики и особенности эксплуатации сетевых средств защиты компьютерной информации;
- сформировать навыки использования сетевых средств защиты информации для реализаций политики информационной безопасности компьютерных систем и сетей

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований сформировавших данную компетенцию
1	Способность осваивать методики использования программных средств для решения практических задач	ОПК-2	Базовый, шестой этап формирования компетенции по аспектам дисциплины	Основы теории информации Системное программное обеспечение
2	Способность разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием	ОПК-3	Базовый, шестой этап формирования компетенции по аспектам дисциплины	Сети и телекоммуникации Сетевые технологии
3	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	ОПК-5	Базовый, шестой этап формирования компетенции по аспектам дисциплины	Защита информации

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяе-	Название дисциплины (модуля), практики, научных исследований для которых

			мый этапом формирования компетенции	данная компетенция является входной
1	Способность осваивать методики использования программных средств для решения практических задач	ОПК-2	Базовый, седьмой этап формирования компетенции по аспектам дисциплины	-
2	Способность разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием	ОПК-3	Базовый, седьмой этап формирования компетенции по аспектам дисциплины	-
3	Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	ОПК-5	Базовый, седьмой этап формирования компетенции по аспектам дисциплины	-

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 осваивать методики использования программных средств для решения практических задач	ОПК-2	принципы реализации централизованной аутентификации в сетях Windows; принципы построения, реализации и размещения систем обнаружения атак;	осуществлять проектирование защищенных компьютерных систем на базе Windows,	Навыками реализации защищенного терминального доступа к компьютерным системам; навыками конфигурирования систем обнаружения атак
2	Способность разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием	ОПК-3	Группы мер защиты информации, используемых при проектировании защищенных компьютерных систем	осуществлять проектирование защищенных компьютерных систем на базе Linux ;инсталлировать, тестировать испытывать соответствующие программно-аппаратные средства защиты	**Владеть** Навыками выбора средств защиты информации в зависимости, от вида обрабатываемой в компьютерной системе информации

3	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-5	механизмы обеспечения безопасности в распределенных вычислительных системах; •	организовать защищенное соединение отдельных сегментов распределенной корпоративной сети	методами формирования требований по защите информации, использовании выбора оптимальной СЗИ с помощью систем анализа риска

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 часов).
Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	8 семестр 144 часов /4 ЗЕ
Лекции (Л)	20
Практические занятия (ПЗ)	4
Лабораторные работы (ЛР)	20
КСР	4
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным работам, рубежному контролю и т.д.)	60
Подготовка и сдача зачета (контроль)	36
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	**Нормативная база по проектированию защищенных компьютерных систем.** Требования по защите информации содержащие сведения, составляющую государственную тайну Приказ ФСТЭК 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации , не составляющей государственной тайны, содержащейся в государственных информационных системах. Приказ ФСТЭК 21 от 18.02.2013. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Приказ ФСТЭК от 14 марта 2014 г. N 31 Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах…»	2	0,6		0,6	4	7,2	Р 6.1№1, гл.2 Р 6.2№3,4,5	*лекция-визуализация*
2	**Проектирование защищенных корпоративных компьютерных систем на базе Windows** Удаленный доступ к компьютерным систем Протоколы удаленного доступа PPP, SLIP. Протоколы аутентификации PAP, SPAP, CHAP,MS-CHAPv2, EAP. Политики удаленного доступа, их структура.	5	0,7	4	0,7	16	26,4	Р 6.1№1, гл. 7	*лекция-визуализация*

	Служба удаленного рабочего стола(УРС) (служба терминалов RDP). Режимы работы УРС в Windows. Принцип работы RDP. Схема лицензирования сервера УРС. Администрирование УРС. Обеспечение безопасности при использовании УРС. Mandatory Integrity Control. Средства мандатного разграничения доступа в современных операционных системах windows. Групповые политики, их состав, использования для защиты и администрирование корпоративных сетей. Наследование групповых политик. Особенности их применения. Реализация аутентификации в корпоративных системах на базе Windows. Основные концепции протокола Kerberos..								
3	**Проектирование защищённых компьютерных систем на базе Linux** Аутентификация пользователей в Linux. Хранение парольной информации. Реализация аутентификации в корпоративных сетях на базе Linux. Использования протокола Kerberos в защищенных компьютерных системах на базе Linux. Особенности реализации дискреционного доступа в Linux системах. Отечественные и зарубежные операционные системы на базе Linux повышенного уровня секретности. Возможности реализации мандатного разграничения доступа в защищенных системах на базе Linux. Встроенные в Linux средства сетевой защиты, обнаружения вторжений и реализации защищенных каналов	3	0,7	8	0,7	10	22,4	Р 6.1№1, гл. 8 Р 6.2 №2, гл. 9	*лекция-визуализация*
4	**Проектирование защищенных корпоративных распределенных компьютерных систем.**	5	0,7		0,7	16	22,4	Р 6.1№1, гл. 9	*лекция-визуализация,*

	Возможности методы защиты информации передаваемой между сегментами распределенной корпоративной сети. Использование виртуальных частных сетей для реализации защищенных корпоративных компьютерных систем. Возможности реализации защищенных сетей на сетевом уровни модели OSI. Набор используемых защищенных протоколов. Способы аутентификации и согласования ключей шифрования в защищенных распределенных корпоративных системах. Реализация защищенных распределенных на презентационном уровни модели OSI. Структура пакетов, организация аутентификации и шифрования. Дополнительные возможности, обеспечиваемые протоколом SSTP. Реализация защищенных виртуальных частных сетей на канальном уровни модели OSI Средства реализации контроля и обеспечение безопасности работы работающих вне офиса сотрудников								
5	**Системы обнаружения вторжений** Нормативная база по системам обнаружения вторжений. Их классификация. Требования, предъявляемые к ним. Способы и места размещения датчиков и агентов. Выявления уязвимостей в компьютерных системах с помощью сканеров уязвимостей. ИХ разновидности и возможности. Этапы осуществления атаки. Общая классификация систем обнаружения атак	3	0,7	4	0,7	7	15,4	Р 6.1 №1, гл. 6 Р 6.2 №1, гл.9	*лекция-визуализация*

	Системы обнаружения вторжений. Возможности, достоинства и недостатки основных их разновидностей. Возможности использования обманных систем. Security Studio Honeypot Manager								
6	**Выбор оптимального состава защищенных компьютерных систем и оптимальных методов защиты информации** Обзор математических методов выбора оптимального варианта реализации системы. Программное обеспечение анализа риска.	2	0,6	4	0,6	7	14,2	Р 6.1 №1, гл. 11	*лекция-визуализация*

Занятия, проводимые в интерактивной форме, составляют 42% от общего количества аудиторных часов по дисциплине.

Практические работы

№ занятия	№ раздела	Тема	Кол-во часов
1-2	1-6	Выступление студентов с докладами по результатам СРС	4

Лабораторные работы

№ занятия	№ раздела	Тема	Кол-во часов
1	2	Сертификаты и сертификационные агенства в Windows Server 2012	4
2	3	Защита корпоративной сети на базе Unix|Linix	4
3	3	Защищенная операционная система Astra Linux Special Edition	4
4	4	Средство комплексного мониторинга информационной безопасности сложных компьютерных систем MaxPatrol	4
5	5	Комплексная система управления информационной безопасностью «Digital Security Office»	4

4. Учебно-методическое обеспечение самостоятельной работы студентов

Формы работы студентов: лекционные занятия, практические занятия, выступление докладов, решение кейс-задач.

Дисциплина «Программно-аппаратные средства защиты информации в ЭВМ и системах» разбита на модули, представляющие собой логически завершенные части курса и являющиеся теми комплексами знаний и умений, которые подлежат контролю.

Контроль освоения тем включает в себя выполнение тестов, защиту лабораторных работ, выполнение кейс-задач и заслушивание докладов по установленным темам

Для максимального усвоения дисциплины рекомендуется проведение письменного тестирования студентов по материалам лекций. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

В качестве организованной самостоятельной работы студента рекомендуется использовать подготовка докладов и презентаций по выбранной заранее тематике и выступление с ними на практических занятиях с последующим их обсуждением. Выступление и обсуждение докладов происходит на 2 практических занятиях. При написании доклада студент должен в соответствии с требованиями к оформлению докладов сформулировать проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения заданной проблемы.

Студенты могут использовать в соответствии с договорами о сотрудничестве УГАТУ с ведущими российскими компаниями в области информационной безопасности лицензионное программное обеспечение данных фирм, установленное в дисплейном классе 5-220 и на серверах кафедры ВТ и ЗИ.

Студенты могут использовать методические указания к выполнению практических и лабораторных работ, решению кейс-задач, документацию по изучаемым программным продуктам, другие электронные источники, расположенные по адресу \\10.40.2.2.\Exchange \ПАЗИ, \\10.40.2.2.\Exchange \ЗИП.

Таблица 5 – Вопросы, выносимые на самостоятельное изучение студентами

№ раздела	Вопросы, выносимые на самостоятельное изучение	Кол-во часов
	2	3
1	Основные понятия Active Directory. Дерево. Лес. Контейнеры. Листья. Контекст имен. Типы имен. Доверительные отношения. Узел, схема, глобальный каталог, публикация. Безопасность Active Directory. Организация репликации. Организация защиты доступа к разделяемым сетевым ресурсам. Протоколы SMB, SMB2. Возможные атаки злоумышленников. Методы повышения уровня защищенности Понятие KDC и сеансовых билетов. Kerberos. Мандаты на выдачу мандатов Аутентификация за пределами домена. Подпротоколы Kerberos. Структура мандатов Kerberos. Компоненты Kerberos Политика безопасности Kerberos. Вход в систему с помощью смарт-карты	12
2	Типы пользователей в Linux. Способы выполнения основные операции с учетными записями. Группы, основные операции с ними. Структура основных конфигурационных файлов Linux	8
3	Протокол SOCKS, схема установления соединения, функции Socks сервера, схемы сетевого взаимодействия по протоколу SOCKS. Особенности реализация защищенных соединений на канальном уровне. Особенности и схемы применения PPTP, L2F, L2TP.	14
4	Обманные системы. Их классификация. Обманная система. Security Studio Honeypot Manager. Отечественные системы анализа защищенности «Ревизор Сети», «Сканер – ВС», MaxPatrol	10
5	Математические методы, лежащие в основе способов выбора оптимальной структуры средств защиты информации. Способы и методика анализа риска, используемые в соответствующем отечественном и зарубежном программном обеспечении	10

Возможные темы докладов:

1) Методические документ ФСТЭК. Меры защиты информации в государственных информационных системах
2) Показателя защищенности и требования к средствам антивирусной защиты
3) Показателя защищенности и требования к электронным замкам
4) Защищенные компьютеры
5) новые возможности защиты информации в Windows Server 2012 R2;
6) сетевые анализаторы;
7) технологии NAP, NAC;
8) сертифицированные средства обнаружения атак;
9) система сертификации межсетевых экранов;
10) система сертификации систем обнаружения вторжений;
11) сканер уязвимостей «Ревизор сети»;
12) IDS Форпост
13) Сети i2p
14) обманная система Security Studio Honeypot Manager;
15) особенности реализации VPN с помощью протокола PPTP;
16) особенности реализации VPN с помощью протокола L2F;
17) реализация VPN с помощью протокола Direct Access;
18) межсетевые шлюзы с поддержкой VPN «Застава»;
19) VPN сети VipNet фирмы Infotecs;
20) VPN сети на оборудовании фирмы Lissi;

21) VPN шлюзы фирмы Checkpoint;
22) особенности защищенных протоколов электронной торговли;
23) особенности защиты информации в электронной торговли;
24) особенности защиты информации в веб-сервере IIS;
25) особенности защиты информации в веб-сервере Apache;
26) защита информации при облачных вычислениях;
27) система защиты средств виртуализации VGate;
28) особенности защиты информации в сетях Machintosh.
29) зарубежные системы анализа риска;
30) реализация VPN встроенными средствами Linux;
31) встроенные в Linux средства межсетевого экранирования.

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)

6.2 Дополнительная 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.Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 N 28375)

4.Приказ ФСТЭК от 11.02.2013 N 17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

5.Приказ ФСТЭК от 14.03.2014 N31. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально важных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

.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	Доступ	Реквизиты договоров с правообладателями

		ресурсов (экз.)		
	2	3	4	5
1.	ЭБС «Лань» http://e.lanbook.com/	41716	С любого компьютера, имеющего выход в Интернет, после регистрации в ЭБС по сети УГАТУ	Договор ЕД-671/0208-14 от 18.07.2014. Договор № ЕД - 1217/0208-15 от 03.08.2015
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	ЭБС создается в партнерстве с вузами РБ. Библиотека УГАТУ – координатор проекта
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	ЭБС создается в партнерстве с аэрокосмическими вузами РФ. Библиотека УГАТУ – координатор проекта
4.	Электронная коллекция образовательных ресурсов УГАТУ http://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	885352 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №1330/0208-14 от 02.12.2014
6	Научная электронная библиотека eLIBRARY* http://elibrary.ru/	9169 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
7	Тематическая коллекция полнотекстовых журналов «Mathematics» издательства Elsevier http://www.sciencedirect.com	120 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Договор №ЭА-190/0208-14 от 24.12.2014 г.

8	Научные полнотекстовые журналы издательства Springer* http://www.springerlink.com	1900 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ открыт по гранту РФФИ
9	Научные полнотекстовые журналы издательства **Taylor& Francis Group*** http://www.tandfonline.com/	1800 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 25.02.2014 г. №14.596.11.0002 между Министерством образования и науки и Государственной публичной научно-технической библиотекой России (далее ГПНТБ России)
10	Научные полнотекстовые журналы издательства Sage Publications*	650 наимен. жрнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 25.02.2014 г. №14.596.11.0002 между Министерством образования и науки и ГПНТБ России
11	Научные полнотекстовые журналы **издательства** Oxford University Press* http://www.oxfordjournals.org/	275 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 25.02.2014 г. №14.596.11.0002 между Министерством образования и науки и ГПНТБ России
12	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 25.02.2014 г. №14.596.11.0002 между Министерством образования и науки и ГПНТБ России

6.4 Методические указания к лабораторным работам

1. Инфраструктура открытых ключей в Windows Server 2012: Методические указания / Уфимск. гос. авиац. техн. ун-т; Сост. В.Е.Кладов. – Уфа, 2015. - 39 с.

2.Защита информационных процессов в операционной системе *Linux/Unix*: Методические указания к лабораторной работе по курсам «Защита информационных процессов в компьютерных системах», «Программно-аппаратные средства защиты информации в ПЭВМ и ВС», «Методы и средства хранения и защиты компьютерной информации»/ Уфимск. гос. авиац. техн. ун-т.; Сост. В. Е. Кладов. – Уфа, 2012. – 31 с.

3.Система управления информационной безопасностью «*Digital Security Office*»: Методические указания к

лабораторной по дисциплинам: «Защита информационных процессов в компьютерных системах», «Программно-аппаратные средства защиты информации в ПЭВМ и ВС», «Методы и средства защиты компьютерной информации», «Методы и средства хранения и защиты информации» / Уфимск. гос. авиац. техн. ун-т; Сост. В. Е. Кладов. – Уфа, 2012. – 38 с.
4.Методические рекомендации по выполнению лабораторных работ 3,4 (в электронном виде, см. Приложение).

6.5 Методические указания к практическим занятиям

Темы докладов и методические указания к ним приведены в разделе 4 данной программы

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
8	Л	Проблемная лекция Лекция-визуализация	2 18
Итого:			20

8. Методические указания по освоению дисциплины

Формы работы студентов: лекционные занятия, лабораторные работы, практические занятия, 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.

Способы контроля освоения тем, фонд оценочных материалов, критерии выставления оценок, доступа к экзамены, критерии оценки на экзамены рассмотрены в разделе 5 настоящей программы

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.

Темы докладов приведены в разделе 4 настоящей программы. Критерии оценки докладов изложены в разделе 5 настоящей программы.

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 могут составляться в электронном виде и должны быть снабжены индивидуальными признаками, подтверждающими выполнение лабораторной работы данной подгруппой. 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. Пройти промежуточное тестирование по окончанию освоения очередного модуля учебной дисциплины.

3. Выступить с докладом.

Критерии доступа к экзамену и получения оценки автоматом представлены в разделе 5 настоящей программы.

Экзамен проводится аудиторно. Студенту задаются 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 i3, 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 ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования);
- программный комплекс – Microsoft Office (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования);
- контур информационной безопасности SearchInform (Лицензионное соглашение с ООО «Новые поисковые технологии UEI-2349-87, 20 пользователей);
- комплексная система управления информационной безопасностью «Digital Security Office»
- операционная система Mindriva (open source)
- операционная система Ubuntu (open source)
- комплексная система управления информационной безопасностью «Digital Security Office»
- операционная система Astra-Linux Special Edition (лицензионный договор с АО «НПО РусБИТех» РБТ-14/1318-01-ВУЗ на предоставление права использования программы для ЭВМ от 29.03.2016 20 лицензий)
- Программное обеспечение Max Patrol Education (лицензионный договор с ЗАО Позитив Технолоджиз 71-16/ЕМ от 21 июня 2016).

10. Адаптация рабочей программы для лиц с ОВЗ

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.