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

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ЭВМ и СИСТЕМАХ»

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 «*Программно-аппаратные средства защиты информации в ЭВМ и системах*» 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 Средства ВТ
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	Средства ВТ 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, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых 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 построения, реализации и размещения систем обнаружения атак;	осуществлять построение централизованной системы защиты корпоративных сетей на базе операционной системы Windows	навыками конфигурирования систем обнаружения атак
2	Способность разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием	ОПК-3	методы защиты информации в беспроводных сетях	инсталлировать, тестировать испытывать программно-аппаратные средства защиты информации вычислительных и информационных систем для операционной системы Linux	навыками настройки систем защиты беспроводных сетей;
3	Способность решать стандартные задачи профессиональной деятельности на ос-	ОПК-5	механизмы обеспечения безопасности в распределенных	организовать защищенное соединение от-	методами формирования требований по защите

	нове информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		вычислительных системах;	дельных сегментов распределенной корпоративной сети	информации, использовани и 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	**Защита корпоративной сети на базе Windows** Основные понятия Active Directory. Дерево. Лес. Контейнеры. Листья. Контекст имен. Типы имен. Доверительные отношения. Узел, схема, глобальный каталог, публикация. Безопасность Active Directory. Организация репликации. Основные концепции протокола Kerberos. 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.	3	0,66	4		7	14,5	Р 6.1№1, гл. 7	*лекция-визуализация*
2	**Защита корпоративной сети на базе Unix|Linux** Версии Unix, Linux. Данные, хранимые в учетной карточке. Месторасположение базы данных учетных записей. Теневые пароли. Шифрование паролей. Утилиты работы с паролями. Принципы работ программ подбора паролей. Способы усиления защиты. Разграничение доступа к объектам на базе Linux, достоинства и недостатки. Флаги. Владелец, группа, права доступа вновь созданного файла. Изменения прав доступа при копировании и перемещении файлов. Сетевая защита в Linux	3	0,67	4		8	15,5	Р 6.1№1, гл. 8 Р 6.2 №2, гл. 9	*лекция-визуализация*
3	**Реализация защищенных распределенных вычислительных систем** Семейства протоколов IPSec. Способы аутентификации, фазы и режимы работы IKE.	7	0,67			4	5,5	Р 6.1№1, гл. 9	*лекция-визуализация,*

	Базы данных безопасных ассоциаций и политик безопасности. Семейство протоколов SSL/TLS. Структура пакетов, организация аутентификации и шифрования. Протокол SSTP Протоколы защищенных сетей на канальном уровне PPTP, L2F, L2TP Direct Access. Назначение, механизмы работы. Технология BranchCache								
4	**Системы обнаружения атак** Классификация удаленных атак на распределенные вычислительные системы. Характеристика и механизмы реализации типовых удаленных атак Причины успеха удаленных атак на распределенные вычислительные системы. Способы защиты от удаленных атак в сети Internet. Этапы осуществления атаки. Общая классификация систем обнаружения атак Средства анализа защищенности. Системы обнаружения атак системного и сетевого уровня. Системы обнаружения атак на уровне узла и на уровне сети. Размещение систем обнаружения атак. Отечественные и зарубежные системы обнаружения атак	3	0,66	8		8	14,5	Р 6.1 №1, гл. 6 Р 6.1 №2, гл. 8-10 Р 6.2 №1, гл.9	*лекция-визуализация*
5	**Системы анализа риска и методы выбора оптимальной СЗИ.** Основные понятия. Стандарты по менеджменту информационной безопасности. Программное обеспечение анализа риска. Методы выбора оптимальной СЗИ	2	0,67	4		6	12	Р 6.1 №1, гл. 11	*лекция-визуализация*

6	**Защита информации в беспроводных сетях** Стандарт аутентификации 802.1x. TKIP, MIC Управление ключами в WPA. Особенности WPA2 Методы защиты информации в сетях сотовой связи *(GSM, CDMA, Bluetooth, 3G, 4G).*	2	0,67		3	9	21	Р 6.1 №1, гл. 12	*лекция-визуализация*

Занятия, проводимые в интерактивной форме, составляют 47% 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	1	Сертификаты и сертификационные агенства в Windows Server 2012	4
2	2	Защита корпоративной сети на базе Unix|Linix	4
3	4	Системы анализа защищенности «Сканер-ВС»	4
4	4	Система комплексного анализа информационной безопасности XSpider	4
5	5	Комплексная система управления информационной безопасностью «Digital Security Office»	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)

6.2 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. 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 (экз.)	Доступ	Реквизиты договоров с правообладателями

	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»
- системы анализа защищенности «Сканер-ВС»(бесплатная версия для учебных заведений)
- система комплексного анализа информационной безопасности XSpider (лицензионный договор с ЗАО Позитив Технолоджиз 71-16/EX от 21 июня 2016).
- Программное обеспечение Max Patrol Education (лицензионный договор с ЗАО Позитив Технолоджиз 71-16/EM 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.