Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

Кафедра «Математическое обеспечение и применение ЭВМ»

УТВЕРЖДАЮ
Первый проректор
_____ И.В. Макурин
«28» 12 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины «Защита информации»

основной профессиональной образовательной программы
подготовки бакалавров
по направлению 09.03.01 - «Информатика и вычислительная техника»
профиль «Программное обеспечение средств вычислительной техники
и автоматизированных систем»

Форма обучения заочная

Технология обучения традиционная

Комсомольск-на-Амуре 2017

Автор рабочей программы _____ М. Е. Щелкунова
доцент, к.т.н. «05» 04 2017 г.

СОГЛАСОВАНО

Директор библиотеки _____ И.А. Романовская
«08» 04 2017 г.

Заведующий кафедрой «МОП ЭВМ» _____ В.А. Тихомиров
«06» 04 2017 г.

Заведующий выпускающей кафедрой «МОП ЭВМ» _____ В.А. Тихомиров
«06» 04 2017 г.

Декан «ФЗДО» _____ М.В.Семибратова
«07» 04 2017 г.

Начальник учебно-методического управления _____ Е.Е. Поздеева
«10» 04 2017 г.

Введение

Рабочая программа дисциплины «Защита информации» составлена в соответствии требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации от 12.01.2016 № 5, и образовательной программы подготовки бакалавров по направлению 09.03.01 «Информатика и вычислительная техника». Данная рабочая программа подготовлена для студентов наборов 2017, 2018 годов и далее.

1 Аннотация дисциплины

<table>
<tr><td>Наименование дисциплины</td><td colspan="6">Защита информации</td></tr>
<tr><td>Цель дисциплины</td><td colspan="6">подготовка студентов к использованию современных методов, средств и технологий защиты компьютерной информации в распределенных корпоративных информационных системах, компьютерных сетях, изолированных системах</td></tr>
<tr><td>Задачи дисциплины</td><td colspan="6">• дать студентам прочные теоретические знания методов и средств защиты компьютерной информации;
• научить студентов практическим навыкам выбора и применения методов и средств защиты компьютерной информации</td></tr>
<tr><td>Основные разделы дисциплины</td><td colspan="6">Основы информационной безопасности. Многоуровневая защита сетей. Практические методы и средства исследования сетей с целью поиска уязвимостей. Защита персональных компьютеров и компьютерных сетей с операционной системой Windows</td></tr>
<tr><td rowspan="4">Общая трудоемкость дисциплины</td><td colspan="6">4 з.е. / 144 академических часов</td></tr>
<tr><td rowspan="2">Семестр</td><td colspan="2">Аудиторная нагрузка, ч</td><td rowspan="2">СРС, ч</td><td rowspan="2">Промежуточная аттестация, ч</td><td rowspan="2">Всего за семестр, ч</td></tr>
<tr><td>Лекции</td><td>Лаб. работы</td></tr>
<tr><td>8</td><td>6</td><td>8</td><td>121</td><td>9</td><td>144</td></tr>
<tr><td>ИТОГО:</td><td>6</td><td>8</td><td>121</td><td>9</td><td>144</td></tr>
</table>

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Дисциплина «Защита информации» нацелена на формирование компетенций, знаний, умений и навыков, указанных в таблице 1.

Таблица 1 – Компетенции, знания, умения, навыки

Наименование и шифр компетенции, в формировании которой принимает участие дисциплина	Перечень формируемых знаний, умений, навыков, предусмотренных образовательной программой		
	Перечень знаний (с указанием шифра)	Перечень умений (с указанием шифра)	Перечень навыков (с указанием шифра)
Способностью 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)	Инструменты обеспечения компьютерной безопасности, З1(ОПК-5-6)	Разворачивать и настраивать программно-аппаратные средства защиты данных, У1(ОПК-5-6)	Навыками выявления узких мест в компьютерной безопасности, Н1(ОПК-5-6)
	Методы и средства обеспечения безопасности данных при работе на компьютере, З2(ОПК-5-6)	Планировать и осуществлять меры по устранению последствий нарушения регламентов обеспечения безопасности, У2(ОПК-5-6)	Навыками планирования работ по устранению последствий нарушения регламентов обеспечения безопасности, Н2(ОПК-5-6)
	Законодательство Российской Федерации в области обеспечения безопасности и защиты персональных данных, З3(ОПК-5-6)	Распознавать факты нарушения регламентов обеспечения безопасности, У3(ОПК-5-6)	Навыками выявления фактов нарушения регламентов обеспечения безопасности, Н3(ОПК-5-6)
	Способы и методы несанкционированного доступа к данным и механизмы противодействия попыткам несанкционированного доступа, З4(ОПК-5-6)	Уметь определять применяемые методы несанкционированного доступа к данным, У4(ОПК-5-6)	Навыками отслеживания несанкционированного доступа к данным и установки защиты данных, Н4(ОПК-5-6)

3 Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» изучается на 4 курсе в 8 семестре.

Дисциплина является обязательной дисциплиной, входит в состав блока Б1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки, сформированные на предыдущих этапах освоения компетенции ОПК-5 «Способностью 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)», в процессе изучения дисциплин:

- этап 1 - Информатика;
- этап 1 - Математический анализ;

- этап 1 - Линейная алгебра и аналитическая геометрия;
- этап 2 - Математический анализ;
- этап 2 - Физика;
- этап 2 - Дискретная математика;
- этап 3 – Учебная практика (исполнительская);
- этап 4 - Математический анализ;
- этап 4 - Физика;
- этап 5 - Теория вероятностей и математическая статистика;
- этап 5 - Физика;
- этап 6 - Математическая логика и теория алгоритмов.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы, 144 академических часа.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов, заочная форма обучения**
Общая трудоемкость дисциплины	144
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	14
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	6
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	8
Самостоятельная работа Обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	121
Промежуточная аттестация обучающихся	9

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость (в часах)	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
Раздел 1 ***Защита информации***					
Тема 1. Основы информационной безопасности Основные понятия и определения информационной безопасности. Источники, риски и формы атак на информацию. Классификация атак на компьютерную информацию. Система защиты информации. Принцип построения системы защиты. Требования к системам защиты информации. Защитные методы и средства. Организационные мероприятия системы защиты информации. Политика безопасности. Физические средства. Технические устройства. Аппаратные средства. Классификация. Программные методы, их состав. Криптография. Криптографические модели. Алгоритмы шифрования. Симметричные, блочные, ассиметричные алгоритмы шифрования данных. Стандарты шифрования данных. Алгоритмы аутентификации пользователей. Простая аутентификация, на основе многоразовых, одноразовых паролей, сертификатов. Биометрическая идентификация и аутентификация пользователя. Строгая аутентификация. Законодательные и правовые аспекты защиты. Виды компьютерных преступлений. Российское законодательство по защите компьютерной информации. Классы безопасности систем. Классификация систем по уровням надежности. Адаптивное управление информационной безопасностью. Технология анализа защищенности. Технологии обнаружения атак. Архитектура и компоненты системы обнаружения атак. Ме-	Лекция	2	Презентационная, с использованием активных методов обучения	ОПК-5	З1(ОПК-5-6), З2(ОПК-5-6), З3(ОПК-5-6), З4(ОПК-5-6)

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость (в часах)	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
тоды реагирования					
Тема 2. Многоуровневая защита сетей Защита персональных компьютеров от несанкционированного доступа к информации. Защита корпоративных сетей. Безопасный обмен данными внутри организации, между внутренними сетями организаций и открытыми сетями. Межсетевые экраны. Классификация, использование, администрирование межсетевых экранов	Лекция	2	Презентационная, с использованием активных методов обучения	ОПК-5	З1(ОПК-5-6), З2(ОПК-5-6), З4(ОПК-5-6)
Тема 3. Практические методы и средства исследования сетей с целью поиска уязвимостей Методы и средства предварительного сбора информации о компьютерных сетях. Методы и средства прослушивания и сканирования компьютерных сетей. Защита от прослушивания и сканирования. Методы и средства инвентаризации сетевых ресурсов, пользователей и групп. Защита от инвентаризации	Лекция	1	Презентационная, с использованием активных методов обучения	ОПК-5	З1(ОПК-5-6), З2(ОПК-5-6), З4(ОПК-5-6)
Тема 4. Защита персональных компьютеров и компьютерных сетей с операционной системой Windows Локальные параметры безопасности. Политика учетных записей. Получение привилегий администратора. Защита от удаленного подбора пароля. Аудит и регистрация событий. Защита системного реестра	Лекция	1	Презентационная, с использованием активных методов обучения	ОПК-5	З1(ОПК-5-6), З2(ОПК-5-6), З4(ОПК-5-6)
Задание 1. Защита компьютера с помощью межсетевого экрана	Лабораторная работа	4	Активная	ОПК-5	У1(ОПК-5-6), У2(ОПК-5-6), У3(ОПК-5-6), У4(ОПК-5-6), Н1(ОПК-5-6),

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость (в часах)	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
					Н2(ОПК-5-6), Н3(ОПК-5-6), Н4(ОПК-5-6)
Задание 2. Защита от атак на компьютер сети с операционной системой Windows	Лабораторная работа	4	Активная	ОПК-5	У1(ОПК-5-6), У2(ОПК-5-6), У3(ОПК-5-6), У4(ОПК-5-6), Н1(ОПК-5-6), Н2(ОПК-5-6), Н3(ОПК-5-6), Н4(ОПК-5-6)
	Самостоятельная работа обучающихся	34	Чтение основной и дополнительной литературы по темам раздела	ОПК-5	З1(ОПК-5-6), З2(ОПК-5-6), З3(ОПК-5-6), З4(ОПК-5-6)
	Самостоятельная работа обучающихся	34	Подготовка к лабораторным занятиям	ОПК-5	З1(ОПК-5-6), З2(ОПК-5-6), З3(ОПК-5-6), З4(ОПК-5-6), У1(ОПК-5-6), У2(ОПК-5-6), У3(ОПК-5-6), У4(ОПК-5-6)

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость (в часах)	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
	Самостоятельная работа обучающихся	53	Выполнение, оформление и подготовка к защите лабораторных работ и расчетно-графической работы	ОПК-5	У1(ОПК-5-6), У2(ОПК-5-6), У3(ОПК-5-6), У4(ОПК-5-6), Н1(ОПК-5-6), Н2(ОПК-5-6), Н3(ОПК-5-6), Н4(ОПК-5-6)
	Текущий контроль		Защита лабораторных работ и расчетно-графической работы	ОПК-5	З1(ОПК-5-6), З2(ОПК-5-6), З3(ОПК-5-6), З4(ОПК-5-6), У1(ОПК-5-6), У2(ОПК-5-6), У3(ОПК-5-6), У4(ОПК-5-6), Н1(ОПК-5-6), Н2(ОПК-5-6), Н3(ОПК-5-6), Н4(ОПК-5-6)
ИТОГО по разделу 1	Лекции	6	-	-	-
	Лабораторные работы	8	-	-	-

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоемкость (в часах)	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
	Самостоятельная работа обучающихся	121	-	-	-
Промежуточная аттестация по дисциплине (экзамен)		9	экзамен	-	-
ИТОГО по дисциплине	Лекции	6	-	-	-
	Лабораторные работы	8	-	-	-
	Самостоятельная работа обучающихся	121	-	-	-
ИТОГО: общая трудоемкость дисциплины 144 часов, в том числе с использованием активных методов обучения 4 часа.					

6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающихся, осваивающих дисциплину «Защита информации», состоит из следующих компонентов: чтение основной и дополнительной литературы по темам дисциплины; подготовка к лабораторным занятиям; выполнение, оформление и подготовка к защите лабораторных работ и расчетно-графической работы, подготовка к экзамену.

Для успешного выполнения всех разделов самостоятельной работы учащимся рекомендуется использовать следующее учебно-методическое обеспечение:

1 Щелкунова М.Е. Комплект электронных УММ для выполнения лабораторных работ и расчетно-графической работы по дисциплине «Защита информации» в локальной сети ФКТ по адресу \\3k316m01\Курс_ЗИ.

2 Методы и средства защиты компьютерной информации : учебное пособие / М. Е. Щелкунова. – Комсомольск-на-Амуре : ФГБОУ ВПО «КнАГТУ», 2005. – 128 с.

3 РД ФГБОУ ВО «КнАГТУ» 013-2016. Текстовые студенческие работы. Правила оформления. – Введ. 2016-03-04. – Комсомольск-на-Амуре : ФГБОУ ВО «КнАГТУ», 2016. – 55 с.

Рекомендуемый график выполнения самостоятельной работы студента в семестре 8 представлен в таблице 4. Время, которым располагает студент для выполнения учебного плана, складывается из двух составляющих: одна из них – это аудиторная работа в вузе по расписанию занятий, другая – внеаудиторная самостоятельная работа. Задания и материалы для самостоятельной работы выдаются во время учебных занятий по расписанию, на этих же занятиях преподаватель осуществляет контроль за самостоятельной работой, а также оказывает помощь студентам по правильной организации работы.

В рамках подготовки к лабораторным занятиям и изучения теоретических разделов дисциплины студенту необходимо проанализировать информацию в сети Интернет и в технической литературе при изучении методов и средств защиты информации. При подготовке к защите лабораторных работ и расчетно-графической работы студенту необходимо обратить внимание на проработку теоретических вопросов по данной теме.

При оформлении отчетов к лабораторным работам и расчетно-графической работе студенту необходимо осуществить поиск, хранение, обработку и анализ информации в сети Интернет и в технической литературе. Так же при оформлении отчетов к лабораторным работам и расчетно-графической работе необходимо строго следовать РД ФГБОУ ВО «КнАГТУ» 013-2016. «Текстовые студенческие работы. Правила оформления».

После успешного выполнения и защиты расчетно-графической работы на лабораторном занятии отчет по расчетно-графической работе студенту необходимо разместить в его личном кабинете, расположенном на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru.

Таблица 4 – Рекомендуемый график выполнения самостоятельной работы студентов заочного отделения в 8 семестре

Вид самостоятельной работы	Часов в неделю																	Итого по видам работ
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
Чтение основной и дополнительной литературы по темам раздела	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**34**
Подготовка к лабораторным занятиям	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**34**
Выполнение, оформление и подготовка к защите лабораторных работ и расчетно-графической работы	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**4**	**3**	**3**	**4**	**3**	**3**	**4**	**3**	**3**	**53**
ИТОГО	**7**	**7**	**7**	**7**	**7**	**7**	**7**	**7**	**8**	**7**	**7**	**8**	**7**	**7**	**7**	**7**	**7**	**121**

7 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Таблица 5 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**	**Показатели оценки**
Тема 1. Основы информационной безопасности	ОПК-5-6	Лабораторные работы (задание 1 - 2), экзамен	Знает методы и средства обеспечения безопасности данных при работе на компьютере. Знает инструменты обеспечения компьютерной безопасности. Знает законодательство Российской Федерации в области обеспечения безопасности и защиты персональных данных. Знает способы и методы несанкционированного доступа к данным и механизмы противодействия попыткам несанкционированного доступа. Умеет планировать и осуществлять меры по устранению последствий нарушения регламентов обеспечения безопасности. Умеет определять применяемые методы несанкционированного доступа к данным. Выявляет узкие места в компьютерной безопасности. Может составить план работ по устранению последствий нарушения регламентов обеспечения безопасности. Демонстрирует навыки выявления фактов нарушения регламентов обеспечения безопас-

			ности, отслеживания несанкционированного доступа к данным и установки защиты данных
Тема 2. Многоуровневая защита сетей	ОПК-5-6	Лабораторная работа (задание 1), экзамен	Знает методы и средства обеспечения безопасности данных при работе на компьютере. Знает инструменты обеспечения компьютерной безопасности. Знает способы и методы несанкционированного доступа к данным и механизмы противодействия попыткам несанкционированного доступа Демонстрирует способность разворачивать и настраивать программно-аппаратные средства защиты данных. Умеет планировать и осуществлять меры по устранению последствий нарушения регламентов обеспечения безопасности. Может распознавать факты нарушения регламентов обеспечения безопасности. Умеет определять применяемые методы несанкционированного доступа к данным. Выявляет узкие места в компьютерной безопасности. Может составить план работ по устранению последствий нарушения регламентов обеспечения безопасности. Демонстрирует навыки выявления фактов нарушения регламентов обеспечения безопасности, отслеживания несанкционированного доступа к данным и установки защиты данных
Тема 3. Практические методы и средства исследования сетей с целью поиска уязвимостей	ОПК-5-6	Расчетно-графическая работа, экзамен	
Тема 4. Защита персональных компьютеров и компьютерных сетей с операционной системой Windows	ОПК-5-6	Лабораторная работа (задание 2), экзамен	

Промежуточная аттестация проводится в 8 семестре в форме экзамена.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, представлены в виде технологической карты дисциплины в таблице 6.

Таблица 6 – Технологическая карта

	Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания**
8 семестр ***Промежуточная аттестация в форме экзамена***				
1	Лабораторные работы (2 работы)	Сессия	20 баллов за одну работу	20 баллов - студент правильно и полностью выполнил практическое задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 15 баллов - студент выполнил практическое задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 10 баллов - студент выполнил практическое задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
2	Расчетно-графическая работа	Сессия	20 баллов	
Итого текущий контроль:			60 баллов	

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
3	Экзамен	Два вопроса –оценивание уровня усвоенных знаний	5 баллов за каждый вопрос	5 баллов - студент правильно ответил на теоретический вопрос билета. Показал отличные знания в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы. 4 баллов - студент ответил на теоретический вопрос билета с небольшими неточностями. Показал хорошие знания в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов. 3 баллов - студент ответил на теоретический вопрос билета с существенными неточностями. Показал удовлетворительные знания в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. 0 баллов - при ответе на теоретический вопрос билета студент продемонстрировал недостаточный уровень знаний. При ответах на дополнительные вопросы было допущено множество неправильных ответов
		Задание практическое – оценивание уровня усвоенных умений	5 баллов	5 баллов - студент правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Ответил на все дополнительные вопросы. 4 балла - студент выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Ответил на большинство дополнительных вопросов. 3 балла - студент выполнил практическое задание билета с существенными неточностями. Показал удовлетворительные умения в рамках освоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. 0 баллов - при выполнении практического задания билета студент продемонстрировал недостаточный уровень умений. При ответах на дополнительные вопросы было допущено множество неправильных ответов
ИТОГО экзамен:			15 баллов	
ИТОГО:			75 баллов	
Критерии оценки результатов обучения по дисциплине: 0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для текущей аттестации по дисциплине); 65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый				

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
(минимальный) уровень); 75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень); 85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

Задания для текущего контроля

Пример задания на лабораторную работу 1

Защита компьютера с помощью межсетевого экрана.

Задание: Проверить защищенность компьютера до установки межсетевого экрана. Установить межсетевой экран на локальном компьютере. Поверить возможности межсетевого экрана по отпору удаленных атак с настройками по умолчанию (имитировать атаки). Настроить межсетевой экран для отпора и регистрации удаленных атак. Имитировать атаки с другого компьютера на удаленный защищенный компьютер для проверки работоспособности межсетевого экрана.

Пример задания на лабораторную работу 2

Защита от атак на компьютер сети с операционной системой Windows.

Задание: Настроить политику учетных записей пользователей. Назначить права пользователей. Настроить параметры безопасности. Для проверки действия установленных параметров: имитировать атаки с другого компьютера на удаленный настроенный компьютер; имитировать атаки на локальном настроенном компьютере. Настроить политику аудита и регистрации событий на локальном компьютере. Назначить объекты (папки, файлы, принтеры), подлежащие аудиту. Настроить, проанализировать информацию журнала безопасности, журнала приложений, системного журнала. Для проверки действия аудита: имитировать атаки с другого компьютера на удаленный настроенный компьютер; имитировать атаки на локальном настроенном компьютере.

Пример задания на расчетно-графическую работу

Прослушивание и сканирование компьютерных сетей.

Задание: Получить открытую информацию об организации и ее служащих. Получить имена и адреса DNS-серверов. Прослушать DNS-серверы. Определить схему компьютерной сети. Предложить меры по обеспечению безопасности информации об организации и баз данных DNS. Прослушать сеть, просканировать порты, определить версии служб и операционной системы, работающих на удаленном компьютере. Предложить меры по защите от прослушивания сети и сканирования портов. Провести инвентаризацию сети. Предложить меры по защите от инвентаризации сети.

Возможные вопросы и задания для защиты работ

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течении срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?
6. В чем преимущество программных генераторов паролей по сравнению с выбором паролей человеком (пользователем либо администратором)?
7. Желательно либо нежелательно, по Вашему мнению, генерирование пароля пользователя на основании некоторого алгоритма из его идентификатора? Повысится либо понизится стойкость защиты при использовании такого алгоритма?
8. В чем состоят минимальные требования к выбору пароля?
9. Что понимается под политикой безопасности в компьютерной системе?
10. В чем заключается модель дискреционной политики безопасности в компьютерной системе?
11. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
12. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?
13. В чем заключается модель мандатной политики безопасности в компьютерной системе?
14. Перечислить группу аксиом, определяющих мандатную модель политики безопасности.
15. Какой уровень допуска должен иметь администратор компьютерной системы?
16. Назначение межсетевых экранов.
17. Особенности функционирования межсетевых экранов.
18. Фильтрующие маршрутизаторы.
19. Шлюзы сеансового уровня.
20. Шлюзы уровня приложений.
21. Методы и средства атак на компьютерные сети с операционной системой Windows.
22. Методы получения привилегий администратора.
23. Защита от удаленного подбора пароля.
24. Политика учетных записей.

25. Параметры политики безопасности в операционной системе Windows.

26. Аудит и регистрация событий.

27. Получение и использование параметров системного реестра.

28. Защита реестра.

29. Получение и использование базы данных SAM.

30. Защита базы данных SAM.

31. Предварительный сбор информации о подключении организации к Internet.

32. Прослушивание серверов DNS.

33. Обеспечение безопасности баз данных DNS.

34. Определение схемы компьютерной сети.

35. Прослушивание компьютерных сетей.

36. Сканирование портов, определение версий служб и операционной системы, работающих на удаленном компьютере.

37. Защита от прослушивания и сканирования компьютерных сетей.

38. Инвентаризация сетевых ресурсов.

39. Инвентаризация пользователей и групп.

40. Защита от инвентаризации.

41. Основные понятия и определения информационной безопасности.

42. Основные причины уязвимости сети Internet.

43. Анализ угроз безопасности корпоративных информационных систем, обусловленных действиями субъектов.

44. Анализ угроз безопасности корпоративных информационных систем, обусловленных техническими средствами и стихийными источниками.

45. Формы сетевых атак на информацию.

Экзаменационные вопросы и задания

В экзаменационном билете – три вопроса. Первый и второй - теоретические вопросы, третий – практическое задание, которое следует выполнить на компьютере.

Возможные вопросы экзаменационного билета

1 Основные понятия и определения информационной безопасности.

2 Основные причины уязвимости сети Internet.

3 Анализ угроз безопасности корпоративных информационных систем, обусловленных действиями субъектов.

4 Анализ угроз безопасности корпоративных информационных систем, обусловленных техническими средствами и стихийными источниками.

5 Формы сетевых атак на информацию.

6 Назначение системы защиты информации.

7 Способы защиты информации.

8 Средства защиты информации.

9 Комплексный подход к решению проблемы защиты информации.

10 Принципы построения системы безопасности.

11 Политика безопасности.

12 Основные понятия и определения криптографической защиты информации.

13 Сравнение схем двух классов криптосистем.

14 Криптоанализ. Определение стойкой криптосистемы.

15 Системы шифрования дисковых данных.

16 Системы шифрования данных, передаваемых по компьютерным сетям.

17 Средства аутентификации электронных данных. Средства управления ключевой информацией.

18 Модель подсистемы информационной безопасности корпоративной сети.

19 Процесс построения подсистемы информационной безопасности корпоративной сети.

20 Модель адаптивного управления безопасностью сети.

21 Средства анализа защищенности всех уровней корпоративной информационной системы.

22 Классификация систем обнаружения атак. Системы обнаружения атак на сетевом и операционном уровнях.

23 Компоненты систем обнаружения атак. Методы анализа информации. Методы реагирования.

24 Стандарты безопасности.

25 Особенности функционирования межсетевых экранов. Использование усиленной аутентификации в межсетевом экране.

26 Фильтрующие маршрутизаторы.

27 Шлюзы сеансового уровня.

28 Шлюзы уровня приложений.

Возможные практические задания экзаменационного билета

1 Методы и средства предварительного сбора информации о подключении организации к Internet. Прослушивание серверов DNS. Обеспечение безопасности баз данных DNS. Определение схемы компьютерной сети.

2 Методы и средства сканирования компьютерных сетей. Прослушивание сети, сканирование портов, определение версий служб и операционной системы, работающих на удаленном компьютере. Защита от прослушивания и сканирования.

3 Методы и средства инвентаризации. Инвентаризация сетевых ресурсов, пользователей и групп. Защита от инвентаризации.

4 Методы и средства атак на компьютерные сети с операционной системой Windows. Получение привилегий администратора. Защита от удаленного подбора пароля. Политика учетных записей.

5 Методы и средства атак на компьютерные сети с операционной системой Windows. Аудит и регистрация событий.

6 Методы и средства атак на компьютерные сети с операционной системой Windows. Использование параметров системного реестра. Защита реестра.

7 Методы и средства атак на компьютерные сети с Windows. Получение и использование базы данных SAM. Защита базы данных SAM.

Примерный вариант экзаменационного билета

1. Основные понятия и определения информационной безопасности.
2. Системы шифрования дисковых данных.
3. Методы и средства предварительного сбора информации о подключении организации к Internet. Прослушивание серверов DNS. Обеспечение безопасности баз данных DNS. Определение схемы компьютерной сети.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

8.1 Основная литература

1 Жук, А. П. Защита информации [Электронный ресурс] : учеб. пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. – 2-е изд. - М. : РИОР : ИНФРА-М, 2018. – 392 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.

2 Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 2-е изд., 3-е изд., 4-е изд., 5-е изд. – СПб. : Питер, 2016; 2011; 2010; 2009; 2004; 2003; 2002; 2001; 2000; 1999. – 992 с.

3 Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : учеб. пособие / Е. К. Баранова. – М. : РИОР : ИНФРА-М, 2013. – 183 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.

8.2 Дополнительная литература

1 Бабаш, А. В. Актуальные вопросы защиты информации [Электронный ресурс] : монография / А. В. Бабаш, Е. К. Баранова. – М. : РИОР : ИНФРА-М, 2017. – 111 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.

2 Бабаш, А. В. История защиты информации в зарубежных странах [Электронный ресурс] : учеб. пособие / Бабаш А. В., Ларин Д. А. – М. : ИЦ РИОР, НИЦ ИНФРА-М, 2016. – 283 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.

3 Бабаш, А. В. Криптографические методы защиты информации. Том 3. [Электронный ресурс] : учебно-методическое пособие / А. В. Бабаш. – 2-е изд. – М. : ИЦ РИОР : НИЦ ИНФРА-М, 2014. – 216 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://www.znanium.com/catalog.php?.

4 Баранова, Е. К. Моделирование системы защиты информации: практикум [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш – М. : ИЦ РИОР : НИЦ ИНФРА-М, 2016 – 120 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://www.znanium.com/catalog.php?.

5 Ларин, Д. А. Криптографическая деятельность в России от Полтавы до Бородина [Электронный ресурс] : монография / Д.А. Ларин. – М. : РИОР : ИНФРА-М, 2017. – 282 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog.php#, ограниченный. – Загл. с экрана.

6 Олифер, В. Г. Сетевые операционные системы: Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2003; 2002; 2001. – 538 с.

7 Хорев, П. Б. Программно-аппаратная защита информации [Электронный ресурс] : учебное пособие / П.Б. Хорев. – 2-е изд., испр. и доп. – М. : Форум: НИЦ ИНФРА-М, 2015. – 352 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://www.znanium.com/catalog.php?.

8 Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. – М. : ИД ФОРУМ : НИЦ ИНФРА-М, 2013. – 592 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://www.znanium.com/catalog.php?.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины (модуля)

1 Единое окно доступа к образовательным ресурсам // Электронный ресурс [Режим доступа: свободный] http://window.edu.ru/.

10 Методические указания для обучающихся по освоению дисциплины (модуля)

Обучение дисциплине «Защита информации» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и лабораторных работ. Самостоятельная работа включает:

- чтение основной и дополнительной литературы по темам дисциплины;

- подготовка к лабораторным занятиям;
- выполнение, оформление и подготовка к защите лабораторных работ и расчетно-графической работы;
- подготовка к экзамену.

Таблица 7 – Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Составление интеллект-карт (MindMap). Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, формулировки, выводы. Отмечать важные мысли. Выделять ключевые слова, термины. Делать пометки на вопросах, терминах, блоках в тексте, которые вызывают затруднения, после чего постараться найти ответ в рекомендуемой литературе. Если ответ не найден, то обратиться к преподавателю
Лабораторная работа	Работа с конспектом лекций (интеллект-картой), просмотр рекомендуемой литературы, работа с интернет-ресурсами, работа с текстом, конспектирование основных мыслей и выводов, выполнение заданий за компьютером
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: изучение теоретических и практических разделов дисциплины; выполнение заданий лабораторных работ; подготовка к защите лабораторных работа; выполнение расчетно-графической работы. Более подробно структура и содержание самостоятельной работы описаны в разделе 6.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. Самостоятельная работа студента направлена на углубление и закрепление знаний студента, развитие практических умений.

Текущий контроль учебной деятельности студентов осуществляется на лабораторных занятиях. Студент обязан в срок выполнять выданные ему лабораторные работы и расчетно-графическую работу. Защита выполненных работ проводится на лабораторном занятии. По результатам сдачи каждой работы присваиваются баллы. Максимальное число баллов за одну лабораторную работу и расчетно-графическую работу – 20. Критерии оценки результатов обучения по дисциплине представлены в технологической карте (таблица 6).

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

В процессе подготовки отчетов к лабораторным и расчетно-графической работам активно используется текстовый процессор.

При изучении дисциплины для выполнения лабораторных работ, расчетно-графической работы рекомендуется использовать следующее свободно распространяемое и лицензионное программное обеспечение и интернет-ресурсы:

- операционная система Windows (Лицензионный сертификат № 46243844 от 09.12.2009);
- Nltest (входит в комплект поставки Microsoft Windows);
- Nslookup (входит в комплект поставки Microsoft Windows);
- RegEdit (входит в комплект поставки Microsoft Windows);
- RegEdt32 (входит в комплект поставки Microsoft Windows);
- Tracert (входит в комплект поставки Microsoft Windows);
- REGDMP (входит в комплект Microsoft Windows Resource Kit Tools, ссылка для свободного скачивания https://www.microsoft.com/en-us/download/details.aspx?id=17657);
- REGINI (входит в комплект Microsoft Windows Resource Kit Tools, ссылка для свободного скачивания https://www.microsoft.com/en-us/download/details.aspx?id 17657);
- SRVINFO (входит в комплект Microsoft Windows Resource Kit Tools, ссылка для свободного скачивания https://www.microsoft.com/en-us/download/details.aspx?id 17657);
- DumpEvt Somarsoft (ссылка для свободного скачивания www.systemtools.com/somarsoft/?somarsoft.com);
- DumpReg Somarsoft (ссылка для свободного скачивания www.systemtools.com/somarsoft/?somarsoft.com);
- DumpSec Somarsoft (ссылка для свободного скачивания 30-дневней пробной версии www.systemtools.com/somarsoft/?somarsoft.com);
- NetScanTools (ссылка для свободного скачивания www.netscantools.com/freeware.html);
- Superscan (ссылка для свободного скачивания superscan.en.softonic.com);
- Winscan (ссылка для свободного скачивания

winscan2pdf.en.softonic.com);

- WS_Ping ProPack (ссылка для свободного скачивания ws-ping-propack.en.softonic.com);
- межсетевой экран Comodo Firewall (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=15);
- межсетевой экран Emsisoft Online Armor Free (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=111);
- межсетевой экран Evorim Free Firewall (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=3241);
- межсетевой экран Jetico Personal Firewall (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=817);
- межсетевой экран Norton Personal Firewall (ссылка для свободного скачивания пробной версии www.securitylab.ru/software/283101.php);
- межсетевой экран Outpost Firewall Pro (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=180);
- межсетевой экран PC Tools Firewall Plus (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=112);
- межсетевой экран TinyWall (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=818);
- межсетевой экран ZoneAlarm Free Firewall (ссылка для свободного скачивания http://www.comss.ru/download/page.php?id=91).
- виртуальная машина VMWare (Лицензия № 954630047 от 8.11.2010, государственный контракт 53-АЭ061, лицензионные ключи);
- антивирусная программа Kaspersky Security Russian Edition 1 year Educational License 1000 Users (продление лицензии; Лицензионный соглашение № 2434-170531-063826-540-363, договор ЕП223/022/20 от 12.05.2017);
- текстовый процессор со свободной лицензией;
- браузер Internet Explorer (компонент операционной системы).

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Для реализации программы дисциплины «Защита информации» используется материально-техническое обеспечение, перечисленное в таблице 7.

Таблица 7 – Материально-техническое обеспечение дисциплины

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование	Назначение оборудования
228/1, 303/3, 303А/3, 305/3, 312/3, 321/3	Компьютерные классы ФКТ	Компьютеры IBM PC Corel-3, 8Мб ОЗУ, Мониторы LCD 17" Acer 11 шт. в классе	Проведение лабораторных занятий

Лист регистрации изменений к РПД

№ п/п	Содержание изменения/основание	Кол-во стр. РПД	Подпись автора РПД
1	Изменение листа подписей в связи со сменой декана ФКТ /пр.№ 271-ЛС «к» от 29.12.2016	1	
2	Изменение КУГ/пр. № 326-О «а» от 04.09.2017	7	
3	Изменение титульного листа в связи с переименованием вуза/пр. №997-О от 03.11.2017	1	
4	Актуализация литературы/ 28.11.2017	2	