

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Новгородский государственный университет имени Ярослава Мудрого»

Институт электронных и информационных систем

Кафедра информационных технологий и систем



ЗАЩИТА ИНФОРМАЦИИ

Модуль для направлений подготовки
09.03.01 – Информатика и вычислительная техника

Рабочая программа

СОГЛАСОВАНО:

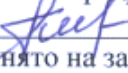
Начальник учебного отдела

 О.Б.Широколобова

« 30 » 11 2017г

Разработал:

Доцент кафедры ИТИС

 С.Ю.Петрова

Принято на заседании кафедры
ИТИС

2. 11. 2017 №2

Зав.кафедрой ИТИС

 А.Я.Гавриков

1 Цели и задачи учебного модуля

Целью учебного модуля «Защита информации» является формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области.

Основные задачи, на решение которых нацелен курс:

- сформировать взгляд на криптографию и защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер;
- изучить базовые теоретические понятия, лежащие в основе процесса защиты информации, сервисы и механизмы безопасности;
- получить представление о компьютерной криптографии, включающей программную реализацию криптографических алгоритмов, проверку их качества, генерацию и распределение ключей, автоматизацию работы по анализу перехвата и раскрытию шифров;
- научиться использованию криптографических алгоритмов шифрования, электронной цифровой подписи, хэш-функций, генерации псевдослучайных последовательностей чисел и протоколов аутентификации, используемых в широко распространенных программных продуктах.

2 Место учебного модуля в структуре ОП направления подготовки

Модуль «Защита информации» входит в базовую часть профессионального цикла Б.3. Формируемые компетенции определяются Федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки бакалавра 09.03.01– Информатика и вычислительная техника.

Освоение дисциплины предполагает знание дисциплин математического и естественно-научного цикла: Информатика, Алгебра и геометрия, Математическая логика и теория алгоритмов, Теория вероятностей и математическая статистика, Дискретная математика, а также знание дисциплин профессионального цикла: Программирование, Алгоритмические языки, Структуры и алгоритмы обработки данных, Базы данных.

Знания в области криптографии и защиты передаваемой, хранимой и обрабатываемой информации, полученные при изучении данного курса, дополняют знания, получаемые при освоении дисциплин: Сети и телекоммуникации, Базы данных, Технологии разработки программного обеспечения, Web-программирование, а также многих дисциплин профессионального цикла БЗ.

3 Требования к результатам освоения учебного модуля

– Способностью решать стандартные задачи профессиональной деятельности на основе информационной¹ и библиографической² культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-5)

¹ Информационная культура личности – это культура поиска новой информации, культура ее восприятия, умение работать с большим объемом сведений, умение сохранять полученную и переработанную информацию, умение четко и доказательно излагать результаты собственной деятельности.

– Способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования (ПК-2)

Код компетенции	Уровень освоения компетенции	Знать	Уметь	Владеть
ОПК-5	базовый	– математические основы криптографии; – организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях; – методы идентификации пользователей; – основы инфраструктуры систем, построенных с использованием публичных и секретных ключей; – методы передачи конфиденциальной информации по каналам связи; – методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).	– применять известные методы и средства поддержки информационной безопасности в компьютерных системах;	– навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;
ПК-2	повышенный	– правовые основы защиты компьютерной информации – – стандарты, модели и методы шифрования	– проводить сравнительный анализ, выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах.	– навыками построения программных систем, содержащих: а) криптографические алгоритмы шифрования передаваемой информации, б) алгоритмы простановки и проверки электронной цифровой подписи, в) алгоритмы хэш-функций, – г) алгоритмы генерации псевдослучайной последовательности чисел

4 Структура и содержание учебного модуля

4.1 Трудоемкость учебного модуля

В структуре УМ выделены следующие учебные элементы модуля (УЭМ) в качестве самостоятельных разделов:

- УЭМ1 Средства защиты от несанкционированного доступа;
- УЭМ2 Криптографические средства.

Учебная работа (УР)	Распределение по семестрам		Коды формируемых компетенций
	Очное обучение 6 сем.	Заочное обучение 7 семестр	09.0301
Трудоемкость модуля в зачетных единицах (ЗЕТ)	3	3	
Распределение трудоемкости по видам УР в академических часах (АЧ):	108	108	ОПК-5, ПК-2
1) УЭМ1 (<i>Средства защиты от несанкционированного доступа</i>):			
	58	58	
- лекции	9	2	
- практические занятия	–	–	
- лабораторные работы	21	5	
- в том числе, аудиторная СРС	4	–	
- внеаудиторная СРС	28	51	
2) УЭМ2 (<i>Криптографические средства</i>):			
	50	50	
- лекции	9	2	
- практические занятия	–	–	
- лабораторные работы	15	3	
- в том числе, аудиторная СРС	5	–	
- внеаудиторная СРС	26	45	
Аттестация: ДЗ	ДЗ	ДЗ	

4.2 Содержание и структура разделов учебного модуля

УЭМ1. Средства защиты от несанкционированного доступа

- 1.1. Информационная безопасность
- 1.2. Средства защиты от несанкционированного доступа
- 1.3. Системы обнаружения и предотвращения вторжений
- 1.4. Системы мониторинга сетей
- 1.5. Антивирусные средства

- 1.6. Межсетевые экраны
- 1.7. Технические средства защиты авторских прав
- 1.8. Запутывание кода программ
- 1.9. Управление ключами. Электронная цифровая подпись

УЭМ2. Криптографические средства

- 2.1. Криптографические средства
- 2.2. Криптографические алгоритмы. Симметричное шифрование
- 2.3. Алгоритм шифрования «РЕЙНДОЛ» (AES)
- 2.4. Алгоритм шифрования ГОСТ 28147-89
- 2.5. Алгоритм шифрования DES
- 2.6. Шифры РИВЕСТА
- 2.7. Алгоритм шифрования «БЛОУФИШ»
- 2.8. Алгоритм шифрования «ТУФИШ»
- 2.9. Алгоритм шифрования «ИДЕА»
- 2.10. Алгоритмы шифрования «ХУФУ» И «ХАФРЕ»
- 2.11. Поточковый алгоритм шифрования «RC4»
- 2.12. Асимметричный алгоритм шифрования RSA
- 2.13. Криптоанализ

Календарный план, наименование разделов учебного модуля с указанием трудоемкости по видам учебной работы представлены в технологической карте учебного модуля (приложение Б).

4.4 Организация изучения учебного модуля

Методические рекомендации по организации изучения УМ с учетом использования в учебном процессе активных и интерактивных форм проведения учебных занятий даются в Приложении А.

5 Контроль и оценка качества освоения учебного модуля

Контроль качества освоения студентами УМ и его составляющих осуществляется непрерывно в течение всего периода обучения с использованием балльно-рейтинговой системы (БРС), являющейся обязательной к использованию всеми структурными подразделениями университета.

Для оценки качества освоения модуля используются формы контроля: текущий – регулярно в течение всего семестра, рубежный и семестровый – по окончании изучения УМ.

Рубежная аттестация на 9 неделе проводится по результатам рубежного контроля по УЭМ. Семестровый – по окончании изучения УМ – осуществляется посредством ДЗ и подсчетом суммарных баллов за весь период изучения УМ. Минимальное количество баллов, необходимое для сдачи экзамена – 75. Максимальное количество баллов – 150.

Оценка качества освоения модуля осуществляется с использованием фонда оценочных средств, разработанного для данного модуля.

Содержание видов контроля и их график отражены в технологической карте учебного модуля (Приложение Б).

Форма	«удовлетворительно»	«хорошо»	«отлично»
Собеседование (защита лабораторных работ) –максимально 3 балла	1,5 – 1,9 балла – испытывает трудности при демонстрации знаний; испытывает трудности в определении терминов и описании алгоритмов действий.	2,0–2,4 балла – допускает неточности при демонстрации знаний; недостаточно четко объясняет значение терминов и описании алгоритмов действий.	2,5 – 3,0 балла – имеет целостное представление материала; четко объясняет значение всех терминов, четко и безошибочно описывает алгоритмы действий.
Индивидуальное собеседование по ауд.СРС; внеауд.СР–ДЗ; рубежный контроль (За одно собеседование максимум 1 балл)	0,5–0,6 баллов испытывает трудности при демонстрации знаний	0,7-0,8 баллов допускает неточности при демонстрации знаний	0,9-1 балл Демонстрирует целостное представление материала
Итоговая аттестация: дифференцированный зачет Максимально 36 балла	18–23 балла испытывает трудности при демонстрации знаний; испытывает трудности в определении терминов и описании алгоритмов действий	24 – 29 баллов – допускает неточности при демонстрации знаний; недостаточно четко объясняет значение терминов и описание алгоритмов действий	30–36 баллов – имеет целостное представление материала; четко объясняет значение всех терминов, четко и безошибочно описывает алгоритмы действий

6 Учебно-методическое и информационное обеспечение

Учебно-методическое и информационное обеспечение учебного модуля представлено Картой учебно-методического обеспечения (Приложение В).

7 Материально-техническое обеспечение учебного модуля

Для осуществления образовательного процесса по дисциплине необходимы:

– для проведения лекций, а также практических занятий – аудитория, оборудованная мультимедийным оборудованием;

Для проведения лабораторных занятий – компьютерные классы с современными ПК и установленным на них лицензионным программным обеспечением. Для выполнения цикла лабораторных работ необходимы компьютеры с установленной операционной системой Microsoft Windows 7 Professional: тип лицензии Microsoft Lreamspark Premium, Dreamspark Order Number: 6002662108; ОС Linux (General Public License); Netfilter (General Public License); ViPNet CSP 4.2. (General Public License); Microsoft Visual Studio Community 2012 (General Public License). Указанное оборудование имеется в распоряжении кафедры ИТиС. Рекомендуемое число компьютеров в учебном классе должно быть не менее 10.

Приложения (обязательные):

А – Методические рекомендации по организации изучения учебного модуля

Б – Технологическая карта

В - Карта учебно-методического обеспечения УМ

Приложение А

А.1 Методические рекомендации по теоретической части учебного модуля

Теоретическая часть модуля направлена на формирование системы знаний в области теории информатики и информационных технологий. Основное содержание теоретической части излагается преподавателем на лекционных занятиях, а также усваивается студентом при знакомстве с дополнительной литературой, которая предназначена для более глубокого овладения знаниями основных дидактических единиц соответствующего раздела и указана в таблице А.1.

А.2 Содержание разделов и тем УМ:

УЭМ1 «Средства защиты от несанкционированного доступа»

Тема 1.1 Информационная безопасность

Цель:изучить основные понятия защиты информации.

Ключевые понятия

Защита информации, информационная безопасность, уровни безопасности, Общие критерии оценки защищённости ИТ, сервисы безопасности, Требования гарантии безопасности.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.1. - Д.3.4.

Тема 1.2 Средства защиты от несанкционированного доступа

Цель:изучить основные средства защиты от несанкционированного доступа.

Ключевые понятия

Предотвращения утечек информации, DLP системы, средства ограничения физического доступа, межсетевое экранирование, системы аутентификации.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 1.

Подготовить ответы на дополнительные вопросы Д.3.5. - Д.3.8.

Тема 1.3 Системы обнаружения и предотвращения вторжений

Цель:изучить системы обнаружения и предотвращения вторжений (IDS/IPS) и системы предотвращения утечек конфиденциальной информации (DLP-системы).

Ключевые понятия

Сетевая COBNetwork-based IDS (NIDS), основанная на протоколе COB (PIDS), основанная на прикладных протоколах COB (APIDS), узловая COBHost-based IDS (HIDS), гибридная COBHybrid IDS, классификация систем предотвращения вторжений, спуфинг, Виды DoSатак, эксплойт, ботнет, межсетевой экран.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.9. - Д.3.14.

Тема 1.4 Системы мониторинга сетей

Цель:изучить системы мониторинга сетей, анализаторы протоколов.

Ключевые понятия

Сниффер, способы перехвата трафика, взлом беспроводных сетей, «Рыбалка» со спутника, средства снижения угрозы сниффинга.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 2.

Подготовить ответы на дополнительные вопросы Д.3.15. - Д.3.19.

Тема 1.5 Антивирусные средства

Цель:изучить программы для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики заражения (модификации) файлов или операционной системы вредоносным кодом.

Ключевые понятия

Классификация антивирусов, сигнатурный метод обнаружения, проактивная защита, полиморфизм компьютерного вируса, эмуляция кода, технология песочницы, виртуализация рабочего окружения, лжеантивирусы.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.20. - Д.3.24.

Тема 1.6 Межсетевые экраны

Цель:изучить возможности межсетевых экранов и проблемы, нерешаемые межсетевым экраном.

Ключевые понятия

Классификация межсетевых экранов по характеристикам, Бэйдор.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 3.

Подготовить ответы на дополнительные вопросы Д.3.25. - Д.3.27.

Тема 1.7 Технические средства защиты авторских прав

Цель:изучить технические средства защиты авторских прав или DRM (Digitalrightsmanagement), программные или программно-аппаратные средства, которые намеренно ограничивают либо затрудняют какие-либо действия с данными в электронной

форме (копирование, модификацию, просмотр ит.п.), либо позволяют отследить такие действия.

Ключевые понятия

Эффективность и правовая основа DRM. Современные технологии DRM

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.28. - Д.3.30.

Тема 1.8 Запутывание кода программ

Цель:изучить способы запутывания кода программ, для предотвращения нарушения авторских прав.

Ключевые понятия

Анализ программного обеспечения, Байт-код шифрование, обфускация имени, стринг шифрование, запутывание потока, антидекомпиляторы, популярные обфускаторы.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 4.

Подготовить ответы на дополнительные вопросы Д.3.31. - Д.3.32.

Тема 1.9. Управление ключами. Электронная цифровая подпись

Цель:изучить роль управления ключами в криптографии, цели управления ключами.

Ключевые понятия

Закрытый ключ. Электронная цифровая подпись. Виды ЭП в РФ. Алгоритмы получения ЭП. Использование хэш-функций. Симметричная и асимметричная схема. Взлом подписей. Подделка документа (коллизия первого рода). Получение двух документов с одинаковой подписью (коллизия второго рода). Социальные атаки. Слепая подпись. Управление открытыми ключами. Хранение закрытого ключа. Политика безопасности. Жизненный цикл ключей

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.33. - Д.3.34.

УЭМ2 «Криптографические средства»

Тема 2.1. Криптографические средства

Цель:изучить методы обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Ключевые понятия

Криптография, принцип Керкгоффса, криптостойкость, шифр Вернама, криптодоказующие программы, устойчивость к брутфорс-атаке, хеширование паролей, атака нахождения прообраза, коллизии криптографических хеш-функции, средства взлома, уязвимость протокола WPS.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 6.

Подготовить ответы на дополнительные вопросы Д.3.35. - Д.3.36.

Тема 2.2. Криптографические алгоритмы. Симметричное шифрование

Цель:изучитьоткрытые алгоритмы шифрования, предполагающие использование вычислительных средств.

Ключевые понятия

Симметричное шифрование, простая перестановка, одиночная перестановка по ключу, перестановка «Магический квадрат», двойная перестановка, требования к симметричным криптосистемам, общая схема симметричных криптосистем, виды симметричных блочных шифров, стандарты шифрования.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 7.

Подготовить ответы на дополнительные вопросы Д.3.37. - Д.3.38.

Тема 2.3. Алгоритм шифрования «РЕЙНДОЛ» (AES)

Цель:изучитьсимметричный алгоритм блочного шифрования AdvancedEncryptionStandard (AES), также известный как Рейндол.

Ключевые понятия

Принцип работы, трансформации, процедура SubBytes, процедура ShiftRows, процедура MixColumns, процедура AddRoundKey, алгоритм обработки ключа, алгоритм выбора раундового ключа, криптостойкость AES, XSL-атака, атака по сторонним каналам.

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.39. - Д.3.40.

Тема 2.4. Алгоритм шифрования ГОСТ 28147-89

Цель:изучитьсоветский и российский стандарт симметричного шифрования, введённый в 1990 году, который также является стандартом СНГ.

Ключевые понятия

Схема работы алгоритма, режим простой замены, гаммирование, режим выработки имитовставки.узлы замены (S-блоки)

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 8.

Подготовить ответы на дополнительные вопросыД.3.41. - Д.3.42.

Тема 2.5. Алгоритм шифрования DES

Цель:изучитьсимметричный алгоритм шифрования DES (DataEncryptionStandard), разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт.

Ключевые понятия

Блочный шифр, преобразования Сетью Фейстеля, циклы шифрования, генерация ключей, конечная перестановка, схема расшифрования, слабые ключи, известные атаки на DES

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.43. - Д.3.44.

Тема 2.6. Шифры РИВЕСТА

Цель:изучитьблочный шифр (длина блока 64 бита) с переменной длиной ключа RC2 (Ron'sCode 2 или Rivest'sCipher 2), разработанный РономРивестом в 1987 году на основе сети Фейстеля.

Ключевые понятия

Описание алгоритма RC5, расширение ключа, свойства алгоритма, варианты алгоритма RC5

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 9.

Подготовить ответы на дополнительные вопросы Д.3.45. - Д.3.46.

Тема 2.7. Алгоритм шифрования «БЛОУФИШ»

Цель:изучитькриптографическийалгоритм Блоуфиш, реализующийблочноесимметричное шифрование.

Ключевые понятия

Алгоритм Блоуфиш, сравнение с симметричными криптосистемами

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.47. - Д.3.48.

Тема 2.8. Алгоритм шифрования «ТУФИШ»

Цель:изучитьсимметричный алгоритм блочного шифрования Twofish с размером блока 128 бит и длиной ключа до 256 бит, разработанный группой специалистов во главе сБрюсом Шнайером.

Ключевые понятия

Алгоритм Twofish, алгоритмОтбеливание, криптопреобразование Адамара, циклический сдвиг на 1 бит, генерация ключей

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 10.

Подготовить ответы на дополнительные вопросы Д.3.49. - Д.3.50.

Тема 2.9. Алгоритм шифрования «ИДЕА»

Цель:изучитьсимметричный блочный алгоритм шифрования данных IDEA (англ. InternationalDataEncryptionAlgorithm, международный алгоритм шифрования данных), запатентованный швейцарской фирмой Ascom.

Ключевые понятия

Алгоритм IDEA, генерация ключей, режимы шифрования, слабые ключи, сравнение с некоторыми блочными алгоритмами

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросыД.3.51. - Д.3.53.

Тема 2.10. Алгоритм шифрования «ХУФУ» И «ХАФРЕ»

Цель:изучитьсимметричныйблочныйкриптоалгоритмKhufu, разработанный Ральфом Мерклом в 1990 году в качестве альтернативы DES, исправляющий ряд ее недостатков.

Ключевые понятия

Алгоритм Khufu, КриптоустойчивостьKhufu и Khafre

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 11.

Подготовить ответы на дополнительные вопросы Д.3.54. - Д.3.56.

Тема 2.11. Поточковый алгоритм шифрования «RC4»

Цель:изучитьпоточковый шифр RC4(также известен какARCFOURилиARC4), широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколахSSLиTLS, алгоритме безопасности беспроводных сетейWEP).

Ключевые понятия

Алгоритм RC4, КриптоустойчивостьRC4, ИнициализацияS-блока, Генерация псевдослучайного словаK, Исследования Руза и восстановление ключа из перестановки, Атака Флурера, Мантина и Шамира, Атака Кляйна, Комбинаторная проблема

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.57. - Д.3.58.

Тема 2.12. Асимметричный алгоритм шифрования RSA

Цель:изучитькриптографический алгоритм с открытым ключом RSA(аббревиатура от фамилий Rivest, Shamir и Adleman), основывающийся на вычислительной сложностизадачи факторизациибольших целых чисел.

Ключевые понятия

Алгоритм RSA, Криптоустойчивость RSA, Создание открытого и секретного ключей, Цифровая подпись, Скорость работы алгоритма RSA, Использование китайской теоремы об остатках для ускорения расшифровки, Атака Винера на RSA, Алгоритм шифрования сеансового ключа

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Подготовить ответы на дополнительные вопросы Д.3.59. - Д.3.60.

Тема 2.13. Криптоанализ

Цель: изучить криптоанализ, как науку о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа.

Ключевые понятия

Криптоанализ. Методы криптоанализа. Атака на основе шифротекста. Атака на основе открытых текстов. Атака на основе подобранного открытого текста. Атака на основе подобранного ключа. Атака «человек посередине». Атака по сторонним каналам. Атака «дней рождений»

Технологии и формы организации

Информационная лекция.

Приёмы: ассоциативный ряд, рассказ, пример, ответы на вопросы.

Задания для самостоятельной работы

Выполнить и сдать на проверку задания аудиторной СРС 12.

Подготовить ответы на дополнительные вопросы Д.3.61. - Д.3.63.

А.3 Методические рекомендации по выполнению лабораторного практикума

Лабораторные занятия по учебному модулю ставят перед собой цель развивать практические навыки работы с современным программным обеспечением ЭВМ.

№ раздела УМ	Наименование лабораторных работ	Трудоемкость, ак. час
1.2	ЛР №1. Применение технологии трансляции сетевых адресов отправителя и получателя в межсетевом экране Netfilter в ОС Linux.	3
1.3	ЛР №2. Программирование алгоритма DES.	3
1.4	ЛР №3. Шифр Виженера.	3
1.5	ЛР №4. Программирование QR.	3
1.6	ЛР №5. Цифровая подпись файла	3
1.7	ЛР №6. Программирование Алгоритма RSA	3
1.8	ЛР №7. Использование средств обфускации программ	3

2.1	ЛР№8. Использование шифровального (криптографического) средства ViPNet CSP 4.2.	3
2.2	ЛР№9. Проверка подлинности и контроль учетных записей UAC в Microsoft Windows 7	3
2.3	ЛР№10. Применение технологии терминального доступа для организации многопользовательского режима обработки информации и удаленного администрирования в Microsoft Windows 7.	3
2.4	ЛР№11. Организация VPN прикладного уровня на основе ОС Windows	2
2.5	ЛР№12. Настройка BitLocker To Go в Microsoft Windows 7	2
2.13	ЛР№13. Анализ устойчивости алгоритмов шифрования WEP и WPA-TKIP	2
		36

Задания для аудиторной самостоятельной работы студентов

Чтобы достичь целей учебного модуля, студенты должны выполнить следующие практические задания.

Аудиторная СРС 1. Необходимо ограничить пользователя компьютера «IN1» в использовании web-сервиса так, чтобы он мог работать только с сервером «OUT2». Обратите внимание на правильную последовательность определения правил фильтрации.

Аудиторная СРС 2. При начальных условиях предыдущей задачи необходимо предоставить внутренним пользователям возможность использования коман-дыPing для проверки доступности внешних узлов, но исключить такую воз-можность для внешних узлов при сканировании узлов защищаемой сети

Аудиторная СРС 3. При начальных условиях предыдущей задачи необходимо предоставить всем клиентам внутренней сети FTP-сервис (рис. 2.10). Учтите, что на рис. 2.10 показан типовой обмен клиента и FTP-сервера, а программа E-Serv, установленная на виртуальных компьютерах, инициализирует передачу данных не с порта 20, а с порта >1024.

Аудиторная СРС 4. При начальных условиях предыдущей задачи необходимо ограничить пользователя компьютера «IN1» в использовании FTP-сервиса так, чтобы он мог работать только с сервером «OUT2»

Аудиторная СРС 5. При начальных условиях предыдущей задачи необходимо предоставить пользователю компьютера «IN1» сервис электронной почты. На компьютере «IN1» приложение OutlookExpress настроено на почтовый ящик с адресом «U1@mail.ru» на сервере «OUT1». Выемка почто-вой корреспонденции осуществляется по протоколу POP3. Произведите от-правку электронного сообщения от имени пользователя U1 самому себе.

Аудиторная СРС 6. При начальных условиях предыдущей задачи необходимо предоставить пользователю внешнего узла «OUT1» возможность работы с внутренним web-сервером «IN1»

Аудиторная СРС 7. При начальных условиях предыдущей задачи необходимо предоставить пользователю внешнего узла «OUT2» возможность работы с внутренним FTP сервером «IN2»

Аудиторная СРС 8. Разработать политику для web-сервера, на котором разрешен только трафик через порты TCP/80 и TCP/443 из любой точки.

Аудиторная СРС 9. Вирус и антивирус. Готовится несколько файлов, часть из которых содержат некие фразы, которые антивирус должен воспринимать как вредоносный код. Антивирус является сервисом, он остаётся запущенным. При открытии/выполнении файлов, содержащих вредоносный код, антивирус блокирует к ним доступ и оповещает об этом пользователя.

Аудиторная СРС 10. Шифратор/ дешифратор. Пользователь вводит текст, выбирает метод шифрования, при необходимости задаёт ключевое слово и другие параметры (в зависимости от шифра). После нажатия кнопки шифрации он видит зашифрованный текст. Затем этот текст может быть дешифрован по нажатию соответствующей кнопки.

Аудиторная СРС 11. Счётчик трафика. Приложение показывает список запущенных процессов, использующих сеть. Также собирает информацию о суммарном количестве входящего трафика по каждому из процессов и всего.

Аудиторная СРС 12. Анализатор трафика. Приложение перехватывает сетевой трафик и анализирует его, отображая в результате следующую информацию: время, IPадрес, порт, протокол, действие.

Задания для внеаудиторная самостоятельная работа студентов

Д.3.1. Сформулируйте понятие информационной безопасности ИС.

Д.3.2. Объясните понятия целостности, конфиденциальности и доступности информации.

Д.3.3. Укажите отличия санкционированного доступа к информации от несанкционированного.

Д.3.4. Перечислите основные признаки классификации возможных угроз безопасности ИС

Д.3.5. Дайте краткую характеристику угрозы безопасности, обозначаемой термином «троянский конь».

Д.3.6. Дайте краткую характеристику угроз безопасности, обозначаемых терминами «вирус» и «червь».

Д.3.7. Назовите и охарактеризуйте наиболее распространенные виды сетевых атак.

Д.3.8. Опишите атаку «человек-в-середине». Какие средства позволяют эффективно бороться с атаками такого типа?

Д.3.9. Опишите атаку типа «отказ в обслуживании» и распределенную атаку «отказ в обслуживании».

Д.3.10. Опишите особенности фишинга и фарминга. Укажите меры противодействия этим атакам.

Д.3.11. Каковы источники нарушений безопасности проводных корпоративных сетей?

Д.3.12. Назовите основные уязвимости и угрозы беспроводных сетей.

Д.3.13. Объясните понятие «политика безопасности организации».

- Д.3.14. Какие разделы должна содержать документально оформленная политика безопасности?
- Д.3.15. Какие проблемы решает верхний уровень политики безопасности?
- Д.3.16. Какие задачи решает средний уровень политики безопасности?
- Д.3.17. Каковы особенности нижнего уровня политики безопасности?
- Д.3.18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
- Д.3.19. Опишите структуру политики безопасности организации.
- Д.3.20. Что представляют собой специализированные политики безопасности?
- Д.3.21. Приведите несколько примеров специальных политик безопасности с описанием их особенностей.
- Д.3.22. Что представляют собой процедуры безопасности?
- Д.3.23. Приведите несколько примеров процедур безопасности с описанием их особенностей,
- Д.3.24. Перечислите основные этапы (разработки политики безопасности организации.
- Д.3.25. Дайте определение понятий «идентификация», «аутентификация», «авторизация», «администрирование».
- Д.3.26. Что понимают под решением задач AAA?
- Д.3.27. Какие задачи решает подсистема управления идентификацией и доступом IAM?
- Д.3.28. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
- Д.3.29. Перечислите основные атаки на протоколы аутентификации.
- Д.3.30. Опишите метод аутентификации на основе многоразовых паролей. Каковы его недостатки?
- Д.3.31. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
- Д.3.32. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
- Д.3.33. Объясните назначение PIN-кода и особенности его использования.
- Д.3.34. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используют для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
- Д.3.35. Опишите функциональность и характеристики смарт-карт и USB-токенов.
- Д.3.36. Опишите методы биометрической аутентификации пользователя.
- Д.3.37. Сформулируйте главную задачу стандартов информационно-безопасности с позиции производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
- Д.3.38. Назовите основные международные стандарты информационной безопасности.
- Д.3.39. Дайте краткую характеристику международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).
- Д.3.40. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности»?
- Д.3.41. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий».
- Д.3.42. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
- Д.3.43. Назовите стандарты информационной безопасности для Интернета
- Д.3.44. Каковы назначение и особенности функционирования протокола SET?

- Д.3.45.** Каковы назначение и функциональность протоколов SSL и IPSec? В чем эти протоколы существенно различаются?
- Д.3.46.** Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?
- Д.3.47.** Перечислите российские стандарты безопасности информационных технологий.
- Д.3.48.** Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основных части этого стандарта.
- Д.3.49.** Дайте определения следующих понятий: криптограмма, крипто алгоритм, криптосистема.
- Д.3.50.** В чем состоит коренное различие симметричных и асимметричных криптосистем?
- Д.3.51.** Охарактеризуйте четыре основных режима работы блочной) алгоритма.
- Д.3.52.** Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.
- Д.3.53.** Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
- Д.3.54.** Сформулируйте концепцию криптосистемы с открытым ключом.
- Д.3.55.** Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.
- Д.3.56.** Каковы особенности однонаправленных функций с секретом?
- Д.3.57.** На чем основывается надежность крипто алгоритма шифрования RSA?
- Д.3.58.** Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
- Д.3.59.** Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.
- Д.3.60.** Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш-функция?
- Д.3.61.** Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
- Д.3.62.** Опишите работы алгоритма Диффи-Хеллмана. Укажите достоинства этого алгоритма.
- Д.3.63.** Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование и инфраструктуры PKI.

Вопросы к дифференцированному зачету

1. Средства защиты от несанкционированного доступа
2. Информационная безопасность
3. Средства защиты от несанкционированного доступа
4. Системы обнаружения и предотвращения вторжений
5. Системы мониторинга сетей
6. Антивирусные средства
7. Межсетевые экраны
8. Технические средства защиты авторских прав
9. Запутывание кода программ
10. Управление ключами. Электронная цифровая подпись
11. Криптографические средства
12. Криптографические алгоритмы. Симметричное шифрование
13. Алгоритм шифрования «РЕЙНДОЛ» (AES)
14. Алгоритм шифрования ГОСТ 28147-89
15. Алгоритм шифрования DES
16. Шифры РИВЕСТА

17. Алгоритм шифрования «БЛОУФИШ»
18. Алгоритм шифрования «ТУФИШ»
19. Алгоритм шифрования «ИДЕА»
20. Алгоритмы шифрования «ХУФУ» И «ХАФРЕ»
21. Поточковый алгоритм шифрования «RC4»
22. Асимметричный алгоритм шифрования RSA
23. Криптоанализ

Таблица А.1 - Организация изучения учебного модуля «Защита информации»

Раздел модуля	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и Интернет-ресурсы
УЭМ1 Средства защиты от несанкционированного доступа			
1.1 Информационная безопасность	– информационная лекция	– Д.3.1. - Д.3.4.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014
1.2 Средства защиты от несанкционированного доступа	– информационная лекция – выполнение ЛРН№1; – собеседование (защита ЛРН№1)	– Аудиторная СРС 1. – Д.3.5. - Д.3.8.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерей-Бибинформ, 2008
1.3. Системы обнаружения и предотвращения вторжений	– информационная лекция	– Д.3.9. - Д.3.14.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерей-Бибинформ, 2008
1.4 Системы мониторинга сетей	– информационная лекция – выполнение ЛРН№2; – собеседование (защита ЛРН№2)	– Аудиторная СРС 2. – Д.3.15. - Д.3.19.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерей-Бибинформ, 2008
1.5 Антивирусные средства	– информационная лекция	– Д.3.20. - Д.3.24.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерей-Бибинформ, 2008

Раздел модуля	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и Интернет-ресурсы
1.6 Межсетевые экраны	– информационная лекция – выполнение ЛР№3; – собеседование (защита ЛР№3)	– Аудиторная СРС 3. – Д.3.25. - Д.3.27.	– Лапониная О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций: Учеб.пособие/Под ред.В.А.Сухомлина. - М.: Интернет-Ун-т Информ.Технологий,2005. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерей-Бибинформ, 2008
1.7 Технические средства защиты авторских прав	– информационная лекция	– Д.3.28. - Д.3.30.	– Лапониная О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций: Учеб.пособие/Под ред.В.А.Сухомлина. - М.: Интернет-Ун-т Информ.Технологий,2005. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерей-Бибинформ, 2008
1.8 Запутывание кода программ	– информационная лекция – выполнение ЛР№4; – собеседование (защита ЛР№4)	– Аудиторная СРС 4. – Д.3.31. - Д.3.32.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерей-Бибинформ, 2008
1.9 Управление ключами. Электронная цифровая подпись	– информационная лекция	– Д.3.33. - Д.3.34.	– Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с.
УЭМ2 Криптографические средства			
2.1 Криптографические средства	– информационная лекция – выполнение ЛР№5; – собеседование (защита ЛР№5)	– Аудиторная СРС 6. – Д.3.35. – Д.3.36.	– Смарт Н. Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. – М. :Техносфера, 2006. – 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. – М. :Либерей-Бибинформ, 2008

Раздел модуля	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и Интернет-ресурсы
Рубежная аттестация		– Выполнить КР(Аудиторная СРС 5.)	
2.2 Криптографические алгоритмы. Симметричное шифрование	– информационная лекция – выполнение ЛРН№6; – собеседование (защита ЛРН№6)	– Аудиторная СРС 7. – Д.3.37. – Д.3.38.	– Смарт Н. Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. – М. :Техносфера, 2006. – 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. – М. :Либерея-Бибинформ, 2008
2.3 Алгоритм шифрования«РЕЙНДОЛ» (AES)	– информационная лекция; – выполнение ЛРН№7; – собеседование (защита ЛРН№7)	– Д.3.39. - Д.3.40.	– Смарт Н. Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. - М. :Техносфера, 2006. - 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерея-Бибинформ, 2008
2.4 Алгоритм шифрования ГОСТ 28147-89	– информационная лекция – выполнение ЛРН№8; – собеседование (защита ЛРН№8)	– Аудиторная СРС 8. – Д.3.41. - Д.3.42.	– Смарт Н. Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. - М. :Техносфера, 2006. - 525с. – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерея-Бибинформ, 2008
2.5 Алгоритм шифрования DES	– информационная лекция – выполнение ЛРН№9; – собеседование (защита ЛРН№9)	– Д.3.43. - Д.3.44.	– Торстейнсон Питер. Криптография и безопасность в технологии.NET = .Netsecurityandcryptography / Пер.сангл.В.Д.Хорева под ред.С.М.Молявко. - М. : БИНОМ. Лаборатория знаний, 2007 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерея-Бибинформ, 2008
2.6 Шифры РИВЕСТА	– информационная лекция	– Аудиторная СРС 9. – Д.3.45. - Д.3.46.	– Торстейнсон Питер. Криптография и безопасность в технологии.NET = .Netsecurityandcryptography / Пер.сангл.В.Д.Хорева под ред.С.М.Молявко. - М. : БИНОМ. Лаборатория знаний, 2007
2.7 Алгоритм шифрования	– информационная лекция	– Д.3.47. - Д.3.48.	– Смарт Н. Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. - М. :Техносфера, 2006. - 525с.

Раздел модуля	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и Интернет-ресурсы
«БЛОУФИШ»	– выполнение ЛРН№10; – собеседование (защита ЛРН№10)		
2.8 Алгоритм шифрования «ТУФИШ»	– информационная лекция	– Аудиторная СРС 10. – Д.3.49. - Д.3.50.	– Мао, Венбо Современная криптография. Теория и практика = Moderncryptography / Пер.сангл.и ред. Д. А .Клюшина. - М.:Вильямс,2005
2.9 Алгоритм шифрования «ИДЕА»	– информационная лекция – выполнение ЛРН№11; – собеседование (защита ЛРН№11)	– Д.3.51. - Д.3.53.	– Сمارт Н. Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. - М. :Техносфера, 2006. - 525с.
2.10 Алгоритмы шифрования «ХУФУ» И «ХАФРЕ»	– информационная лекция	– Аудиторная СРС 11. – Д.3.54. - Д.3.56.	– Смарт Н. Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. - М. :Техносфера, 2006. - 525с.
2.11 Поточковый алгоритм шифрования «RC4»	– информационная лекция	– Д.3.57. - Д.3.58.	– Мао, Венбо Современная криптография. Теория и практика = Moderncryptography / Пер.сангл.и ред. Д. А .Клюшина. - М.:Вильямс,2005
2.12 Асимметричный алгоритм шифрования RSA	– информационная лекция – выполнение ЛРН№12; – собеседование (защита ЛРН№12)	– Д.3.59. - Д.3.60.	– Бернет Стив. Криптография.Официальное руководство RSA Security / Пер.сангл.подред.А.И.Тихонова. - М. : Бином, 2007
2.13 Криптоанализ	– информационная лекция – выполнение ЛРН№13; – собеседование (защита ЛРН№13)	– Аудиторная СРС 12. – Д.3.61. - Д.3.63.	– Мао, Венбо Современная криптография. Теория и практика = Moderncryptography / Пер.сангл.и ред. Д. А .Клюшина. - М.:Вильямс,2005 – Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. :Либерия-Бибинформ, 2008

Раздел модуля	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и Интернет-ресурсы
Итоговая аттестация (дифференцированный зачет)	ДЗ	– подготовиться к итоговой аттестации	

Приложение Б
Технологическая карта
учебного модуля «Защита информации»
семестр __6__, ЗЕТ_3__, вид аттестации _дифференцированный зачет, акад.часов_108, баллов рейтинга_150

№ и наименование раздела учебного модуля, КП/КР	№ неде- ли сем.	Трудоемкость, ак.час					Форма текущего контроля успеv. (в соотv. с паспортом ФОС)	Максим. кол-во баллов рейтинга
		Аудиторные занятия				СРС		
		ЛЕК	ПЗ	ЛР	АСРС			
УЭМ1 Средства защиты от несанкционированного доступа:		9,0	0,0	21,0	4,0	28,0		48
1.1 Информационная безопасность	1	1,0				4,0	собеседование (защита) Д.3.1. - Д.3.4.	4
1.2 Средства защиты от несанкционированного доступа	2	1,0		3,0	1,0	4,0	собеседование (защита) – Аудиторная СРС 1. Д.3.5. - Д.3.8. собеседование (защита ЛРН№1)	1+4+3
1.3. Системы обнаружения и предотвращения вторжений	3	1,0		3,0		4,0	собеседование (защита) Д.3.9. - Д.3.14.	6
1.4 Системы мониторинга сетей	3	1,0		3,0	1,0	4,0	собеседование (защита) – Аудиторная СРС 2. Д.3.15. - Д.3.19. собеседование (защита ЛРН№2)	1+5+3
1.5 Антивирусные средства	4	1,0		3,0		2,0	собеседование	

							(защита) Д.3.20. - Д.3.24.	5
1.6 Межсетевые экраны	4	1,0		3,0	1,0	2,0	собеседование (защита) – Аудиторная СРС 3. Д.3.25. - Д.3.27. собеседование (защита ЛРН№3)	1+3+3
1.7 Технические средства защиты авторских прав	5	1,0		3,0		2,0	собеседование (защита) Д.3.28. - Д.3.30.	3
1.8 Запутывание кода программ	6	1,0		3,0	1,0	2,0	собеседование (защита) – Аудиторная СРС 4. Д.3.31. - Д.3.32. собеседование (защита ЛРН№4)	1+2+3
1.9 Управление ключами. Электронная цифровая подпись	7	1,0				4,0	собеседование (защита) Д.3.33. - Д.3.34.	2
УЭМ2 Криптографические средства:		9,0	0,0	15,0	5,0	26,0		
2.1 Криптографические средства	8	1,0		3,0	0,5	2,0	собеседование (защита) Аудиторная	1+2+3

							СРС 6. Д.3.35. - Д.3.36. собеседование (защита ЛРН№5)	
Рубежный контроль	9				0,5		выполнить КР (Аудиторная СРС 5.)	1
2.2 Криптографические алгоритмы. Симметричное шифрование	9	1,0		3,0	0,5	2,0	собеседование (защита) – Аудиторная СРС 7. – Д.3.37. - Д.3.38. – собеседован ие (защита ЛРН№6)	1+2+3
2.3 Алгоритм шифрования «РЕЙНДОЛ» (AES)	9	1,0		3,0		2,0	собеседование (защита) Д.3.39. - Д.3.40. собеседование (защита ЛРН№7)	2+3
2.4 Алгоритм шифрования ГОСТ 28147-89	10	0,5		2,0	0,5	2,0	собеседование (защита) – Аудиторная СРС 8. Д.3.41. - Д.3.42. собеседование (защита ЛРН№8)	1+2+3
2.5 Алгоритм шифрования DES	10	0,5		2,0		2,0	собеседование (защита)	2+3

							Д.3.43. - Д.3.44. собеседование (защита ЛРН№9)	
2.6 Шифры РИВЕСТА	11	0,5			0,5	2,0	собеседование (защита) – Аудиторная СРС 9. Д.3.45. - Д.3.46.	1+2
2.7 Алгоритм шифрования «БЛОУФИШ»	12	0,5				2,0	собеседование (защита) Д.3.47. - Д.3.48. собеседование (защита ЛРН№10)	2+3
2.8 Алгоритм шифрования «ТУФИШ»	13	0,5			0,5	2,0	собеседование (защита) – Аудиторная СРС 10. Д.3.49. - Д.3.50.	1+2
2.9 Алгоритм шифрования «ИДЕА»	14	0,5				2,0	собеседование (защита) Д.3.51. - Д.3.53. собеседование (защита ЛР11)	3+3
2.10 Алгоритмы шифрования «ХУФУ» И «ХАФРЕ»	15	0,5			1,0	2,0	собеседование (защита) – Аудиторная СРС 11. Д.3.54. -	1+3

							Д.3.56.	
2.11 Поточный алгоритм шифрования «RC4»	16	0,5				2,0	собеседование (защита) Д.3.57. - Д.3.58.	2
2.12 Асимметричный алгоритм шифрования RSA	17	1,0				2,0	собеседование (защита) Д.3.59. - Д.3.60. собеседование (защита ЛР№12)	2+3
2.13 Криптоанализ	18	1,0		2,0	1,0	2,0	собеседование (защита) – Аудиторная СРС 12. Д.3.61. - Д.3.63. собеседование (защита ЛР№13)	1+3+3
Итоговая аттестация	18						Дифференциро ванный зачет	36
Итого:		18,0	0,0	36,0	9,0	54,0		150,0

Критерии оценки качества освоения студентами дисциплины

В соответствии с Положением «Об организации учебного процесса по образовательным программам высшего профессионального образования» и «О фонде оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации студентов, итоговой аттестации выпускников»:

- оценка «удовлетворительно» – 75-104;
- оценка «хорошо» – 105-134;
- оценка «отлично» – 135-150.

Приложение В

Карта учебно-методического обеспечения

Учебного модуля Защита информации

Направление (специальность) 09.0301

Формы обучения очная

Курс 3 Семестр 6

Часов: всего 3 ЗЕ, лекций 18, лаб. раб. 36, СРС 54

Обеспечивающая кафедра, ИТиС

Таблица 1- Обеспечение учебного модуля учебными изданиями

Библиографическое описание* издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	Наличие в ЭБС
Учебники и учебные пособия		
Мельников В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с.	2	
Лапони́на О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций: Учеб.пособие/Под ред.В.А.Сухомлина. - М.: Интернет-Ун-т Информ.Технологий,2005.-604	2	
Смарт Н.Криптография / Пер.сангл.С.А.Кулешова под ред.С.К.Ландо. - М. : Техносфера, 2006. - 525с.	9	
Бернет Стив.Криптография.Официальное руководство RSA Security / Пер.сангл.подред.А.И.Тихонова. - М. : Бином, 2007. - 381,[1]с.	1	
Мао, Венбо Современная криптография. Теория и практика = Modern cryptography / Пер.сангл.и ред. Д. А .Клюшина. - М.:Вильямс,2005.-763с	3	
Учебно-методические издания		
Арутюнов В. В. Защита информации : учеб.-метод. пособие. - М. : Либерия-Бибинформ, 2008. - 55,[1]с.	1	
Петрова С.Ю. Рабочая программа учебного модуля «Защита информации». – В.Новгород, НовГУ, 2015. – 28с.		1

Таблица 2 – Информационное обеспечение учебного модуля

Название программного продукта, интернет-ресурса
[Электронный ресурс]: ГОСТ Р 50922-2006 «Защита информации» – Режим доступа: WWW.URL: http://www.altell.ru/legislation/standards/50922-2006.pdf
[Электронный ресурс]: Журнал «Защита информации. Инсайд» – Режим доступа: WWW.URL: http://www.inside-zi.ru/

Таблица 3 – Информационное обеспечение УМ дополнительной литературой

Библиографическое описание* издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	Наличие в ЭБС
Проектирование инфраструктуры ActiveDirectory и сети на основе MicrosoftWindowsServer 2003 = Designing a MicrosoftWindowsserver 2003 ActiveDirectoryandnetworkinfrastructure : экзамен 70-297 MCSE : учеб. курс Microsoft : пер. с англ. / Авт.: Уолтер Гленн при участии Майкла Т. Симпсона. - М.; СПб. : Русская редакция: Питер, 2006. - 341, [1] с.	1	
Торстейнсон Питер. Криптография и безопасность в технологии.NET = .Netsecurityandcryptography / Пер. сангл. В. Д. Хорева под ред. С. М. Молявко. - М. : БИНОМ. Лаборатория знаний, 2007. - 479 с.	1	

Действительно для учебного года 2017-2020

Зав. кафедрой

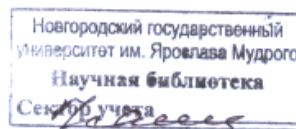


А.Л. Гавриков

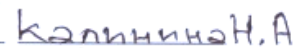
СОГЛАСОВАНО

НБ НовГУ:


должность



подпись


расшифровка