РАБОЧАЯ ПРОГРАММА

Дисциплина:	Информационная безопасность
Кафедра:	Кафедра цифровой экономики
	(ЦЭ) аббревиатура

Специальность (направление) 38.03.05 «Бизнес-информатика»
(код специальности (направления), полное наименование)

.

Сведения о разработчиках:

ФИО	Аббревиатура кафедры	Ученая степень, звание
Сковиков Анатолий Геннадьевич	ЦЭ	к.т.н., доцент

Дисциплина «Информационная безопасность» посвящена изучению основ информационной безопасности. Рассматриваются основные понятия информационной безопасности, структура мер в области информационной безопасности, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. Рассматриваются виды угроз информационной безопасности; методы и средства борьбы с угрозами информационной безопасности; понятие политики безопасности, существующие типы политик безопасности; действующие стандарты информационной безопасности; нормативные руководящие документы.

Цель дисциплины – формирование у будущих специалистов и руководителей системных знаний по проблеме обеспечения комплексной защиты информационных ресурсов и управлению информационными рисками, а также практических навыков безопасной работы в информационных системах.

Задачи дисциплины:

- формирование системных представлений об управлении информационными рисками;
- изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;
- формирование практических навыков анализа защищенности информационных систем, использования встроенных возможностей ОС, MS Office, Брандмауэра Windows, Internet Explorer, а также антивирусных и криптографических средств для обеспечения безопасности информации;
- получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;
- изучение проблем защиты информации, стоящих перед современной вычислительной техникой;
- формирование навыков использования полученных знаний для правильного выбора решений при разработке криптографических, организационных, технических средств защиты информации.

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина «Информационная безопасность» принадлежит вариативной части ФГОС ВО по направлению «Бизнес-информатика». Дисциплина изучается студентами второго курса бакалавриата. Шифр дисциплины в рабочем учебном плане – Б1.В.ОД.2.

Дисциплина занимает особое место в учебном плане. Вместе с курсами по программированию, курс «Информационная безопасность» составляет основу образования студента в части ООП, касающейся современных информационных технологий и обеспечения безопасности информационных систем.

Дисциплина рассчитана на студентов, имеющих подготовку по предшествующим курсам, касающихся основ программирования с использованием алгоритмических языков, алгебры и теории чисел, теории вероятности. Предполагается, что студенты знакомы с основными понятиями алгебры, комбинаторики, теории вероятности, информатики, которые изучаются в рамках данной ООП перед изучением данной дисциплины.

Изучение курса «Информационная безопасность» базируется на компетенциях, сформированных у обучающихся в процессе изучения дисциплин:

- "Вычислительные системы, сети, телекоммуникации";
- "Право";
- "Информационные системы и технологии".

Базовые фундаментальные знания, полученные при изучении курса "Информационная безопасность", позволяют перейти к изучению дисциплин:

- "Электронный бизнес";
- "Информационные системы управления производственной компанией".

Знания, навыки и умения, приобретенные в результате прохождения курса, будут востребованы при выполнении курсовых и выпускной квалификационной работ, связанных с обеспечением защиты информационных систем, ИТ-инфраструктуры, безопасной работы в сети Интернет.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины формируются следующие компетенции:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1);
- организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия (ПК-9).

В результате освоения дисциплины студенты должны:

Иметь представление:

- о критериях оценки защищенности систем;
- о проблемах и направлениях развития аппаратных и программных средств защиты информации;
- о современных криптографических системах.

Знать:

- понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;
- стандартные программные средства набора текста и баз данных;
- правовые акты в области защиты государственной тайны и информационной безопасности;
- правовые основы организации защиты государственной тайны и конфиденциальной информации;
- основные понятия информационной безопасности;
- основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках;
- возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ;
- основные принципы организации и алгоритмы функционирования операционных систем и оболочек;
- проблемы и направления развития системных программных средств.

Уметь:

- использовать программные и аппаратные средства персонального компьютера;
- ориентироваться в современной системе источников информации;
- использовать современные информационные технологии в своей профессиональной деятельности;

- применять средства антивирусной защиты;
- анализировать информационную безопасность многопользовательских систем;
- пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;
- видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи.

Приобрести навыки:

- обеспечения безопасной работы на компьютере;
- поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами;
- современной терминологией и методологией в области информационной безопасности.

Владеть, иметь опыт:

- применения аппаратных и программных средств обеспечения информационной безопасности;
- противостояния типовым удаленным атакам.

Дисциплина предполагает формирование навыков построения комплексной защиты информационных сервисов и ресурсов, применения стандартных программно-аппаратных средств обеспечения информационной безопасности.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Объём дисциплины в зачетных единицах (всего): *5 зачетных единиц (180 часов).*

3.2. Объём дисциплины по видам учебной работы (в часах)

Вид учебной работы	**Всего часов**
Общая трудоемкость базового модуля дисциплины	180
Аудиторные занятия (всего)	72
В том числе:	
Лекции	18
Семинары	36
Лабораторные работы	18
Самостоятельная работа	63
В том числе:	
Творческая работа (эссе)	-
Подготовка опорного конспекта по разделу	-
И (или) другие виды самостоятельной работы	63
Вид промежуточного контроля	-
Вид итогового контроля	Экзамен

3.3 Содержание дисциплины. Распределение часов по темам и видам учебной работы

№ п/п	Раздел Дисциплины	Семестр	Неделя семестра	Общая трудоёмкость (в часах)	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости Форма промежуточной аттестации
					Учебная работа			В.т.ч. интерактив. формы	Самостоятельная работа	
				всего	лекции	практ.	лаб.раб.			
1.	**Раздел № 1. Введение в информационную безопасность.**	3	1-2	12	2				10	Опрос, решение задач, опорный конспект
2.	**Раздел № 2. Классификация и характеристика угроз безопасности информации.**	3	3-4	19	2	12		2	5	Опрос, решение задач, опорный конспект
3.	**Раздел № 3. Стандарты и спецификации в области информационной безопасности.**	3	5-6	4	2				2	Опрос, решение задач, опорный конспект
4.	**Раздел № 4. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности.**	3	7-8	4	2				2	Опрос, решение задач, опорный конспект
5.	**Раздел № 5. Идентификация и аутентификация, управление доступом.**	3	9-10	18	2	4	8	4	4	Опрос, решение задач, опорный конспект
6.	**Раздел № 6. Методы криптографической защиты информации.**	3	11-12	28	2	6	4	2	16	Опрос, решение задач, опорный конспект, тестирование
7.	**Раздел № 7. Протоколирование и аудит, контроль целостности.**	3	13-14	12	2	2	4		4	Опрос, решение задач, опорный конспект
8.	**Раздел № 8. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование и управление**	3	15-16	14	2	8		2	4	Опрос, решение задач, опорный конспект
9.	**Раздел № 9. Защита**	3	17-18	24	2	4	2		16	Опрос,

	компьютерных систем от вирусов и вредоносных программ.									решение задач, опорный конспект, тестирование
	Подготовка к экзамену	3		45						
	ИТОГО:	**-**	**-**	**180**	**18**	**36**	**18**	**10**	**63**	**Экзамен 3 семестр**

4. СОДЕРЖАНИЕ КУРСА

№	Наименование раздела дисциплины	Содержание раздела дисциплины	Результат обучения, формируемые компетенции
1.	**Введение в информационную безопасность.**	Основные понятия: задачи, объект, предмет, методы информационной безопасности. Политика в сфере обеспечения информационной безопасности России. Концептуальная модель информационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Федеральный закон «О государственной тайне». Федеральный закон «О персональных данных». Федеральный закон «Об электронной подписи». Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года. Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации. Сведения и данные, отличие от информации. Информация по уровню доступа. Конфиденциальность информации. Понятие конфиденциальной информации. Классификация конфиденциальной информации. Понятие государственной тайны. Степени грифа секретности. Виды сведений составляющих государственную тайну. Перечень информации, не подлежащей к засекречиванию. Классификация видов профессиональной тайны и объекты их приложения.	Знает: основные понятия, изложенные в Доктрине информационной безопасности РФ и Федеральном Законе «Об информации, информационных технологиях и защите информации»; интересы личности, общества и государства в информационной области; понятие ценности информации, защиты информации, системы защиты информации; цели и концептуальные основы защиты информации; основные виды угроз безопасности информации и их классификацию. Умеет: производить анализ типов информации в зависимости от порядка ее предоставления; делать разбор методов обеспечения информационной безопасности; классифицировать в соответствии с уровнями обеспечения национальной безопасности группы субъектов; подразделять основные средства защиты по видам деятельности; пользоваться в своей профессиональной деятельности основными нормативными правовыми актами в сфере обеспечения информационной безопасности. Владеет: понятиями «информатизация», «информационные технологии», «информационная безопасность», «национальная безопасность», «доктрина информационной

			безопасности»; методами классификации конфиденциальной информации; навыками работы с документами в сфере обеспечения информационной безопасности.
2.	**Классификация и характеристика угроз безопасности информации.**	Понятие угроз безопасности. Классификация угроз информационной безопасности. Основная классификация угроз: угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения доступности информации. Методы перечисления угроз. Случайные и преднамеренные угрозы. Технологические возможности злоумышленников по преодолению систем защиты информации. Признаки угрозы безопасности информации в распределенных вычислительных системах (РВС): по характеру воздействия; по цели воздействия; по условию начала осуществления воздействия; по наличию обратной связи с атакуемым объектом; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие. Характеристика и механизмы реализации типовых удаленных атак. Понятие типовой удаленной атаки. Анализ сетевого трафика. Подмена доверенного объекта или субъекта РВС. Ложный объект РВС. Внедрение в РВС ложного объекта путем навязывания ложного маршрута. Внедрение в РВС ложного объекта путем использования недостатков алгоритмов удаленного поиска. Использование ложного объекта для организации удаленной атаки на РВС. Селекция потока информации и сохранение ее на ложном объекте РВС. Модификация информации. Подмена информации. Отказ в обслуживании.	Знает: понятие угроз безопасности; способы классификации угроз информационной безопасности; технологические возможности злоумышленников по преодолению систем защиты информации; характеристики и механизмы реализации типовых удаленных атак; понятие типовой удаленной атаки; уязвимости сетевых протоколов ARP, ICMP, DNS, TCP, FTP, TELNET; принципы создания защищенных систем связи в распределенных вычислительных системах. Умеет: классифицировать угрозы безопасности информации в распределенных вычислительных системах. Владеет: основными сетевыми командами ОС Windows, используемыми для обеспечения безопасности распределенных вычислительных систем.
3.	**Стандарты и спецификации в области информационной безопасности.**	Понятие стандарта. Классификация стандартов в области информационной безопасности. «Оранжевая книга», ее структура и группы классов защищенности. Руководящие документы Гостехкомиссии России. Понятие несанкционированного доступа (НСД). Направления защиты от НСД. Основные способы НСД. Принципы защиты от НСД.	Знает: классификацию стандартов в области информационной безопасности; руководящие документы Гостехкомиссии России; направления защиты от несанкционированного доступа. Умеет: оперировать терминологией и методологией

		Классификация нарушителей. Понятие системы разграничения доступа (СРД). Основные функции СРД. Тезисы из руководящего документа «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации». Тезисы из руководящего документа «Автоматизированные системы. Защита от НСД к информации. Основные идеи документа «Общие критерии» ISO/IEC 15408-1999. Понятие профиля защиты (ПЗ) и Задания по безопасности (ЗБ). Основные положения международного стандарта ISO/IEC 17799:2005. Основные положения международного стандарта ISO/IEC 27001:2005. Основные положения британского стандарта BS 7799-3:2006.	информационной безопасности, изложенными в «Оранжевой книге». Владеет: основными идеями документа «Общие критерии» ISO/IEC 15408-1999, понятиями профиля защиты и задания по безопасности.
4.	**Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности.**	Уровни защиты информации. Ключевые понятия информационной безопасности - политика безопасности и программа безопасности. Структура соответствующих документов, меры по их разработке и сопровождению. Этапы жизненного цикла информационных систем и меры безопасности. Методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств. Оценка рисков: выбор анализируемых объектов и уровня детализации их рассмотрения; выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий, выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска. Основные классы мер процедурного уровня: управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ.	Знает: структуру политики безопасности и программы безопасности, меры по их разработке и сопровождению; способы оценки рисков. Умеет: выбирать методологии оценки рисков; анализировать угрозы и их последствий; выявлять уязвимые места в защите; оценивать риски; выбирать защитные меры. Владеет: методами и способами управления персоналом; организации физической защиты; поддержания работоспособности; реагирования на нарушения режима безопасности; планирования восстановительных работ.
5.	**Идентификация и аутентификация, управление доступом.**	Техническое обеспечение информационной безопасности. Понятие сервиса безопасности. Понятие архитектурной безопасности. Классификация сервисов безопасности. Средства идентификации и аутентификации пользователей. Идентификация и аутентификация, управление доступом. Парольная аутентификация. Одноразовые пароли. Система S/KEY	Знает: понятие сервиса безопасности; понятие архитектурной безопасности; назначение списков управления доступом; принципы функционирования системы S/KEY и сервера аутентификации Kerberos. Умеет: проектировать и использовать средства

		компании Bellcore. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Матрица доступа. Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом. Ограничивающий интерфейс. Ролевое управление доступом. Статическое разделение обязанностей. Динамическое разделение обязанностей.	идентификации и аутентификации пользователей. Владеет: идеологией произвольного (дискреционного) управления доступом, принудительного (мандатного) управления доступом, ролевого управления доступом.
6.	**Методы криптографической защиты информации. Электронная цифровая подпись.**	Основные понятия и классификация средств криптографической защиты информации. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Основные свойства асимметричных криптосистем. Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Основные свойства хэш-функций. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи. Схемы неоспоримой подписи. Защита информации при работе в сети Интернет.	Знает: основные понятия и классификацию средств криптографической защиты информации; различия между стеганографией и криптографией; основные методы симметричного шифрования; основные методы построения асимметричных криптосистем. Умеет: использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; использовать алгоритмы генерации, хранения и распределения ключей. Владеет: технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.
7.	**Протоколирование и аудит, контроль целостности.**	Протоколирование и аудит, их место в общей архитектуре безопасности. Активный аудит. Подозрительная активность. Сигнатура атаки. Функциональные компоненты, входящие в состав средств активного аудита. Применение аудита в ОС семейства Windows для отслеживания	Знает: место и роль протоколирования в общей архитектуре безопасности; место и роль аудита в общей архитектуре безопасности. Умеет: использовать методы активного аудита. Владеет: инструментами ОС семейства Windows для

		деятельности пользователей. Настройка политики аудита. Аудит в Windows Server 2008/2012.	настройка политики аудита.
8.	**Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование.**	Основные понятия. Понятие демилитаризованной зоны. Механизмы защиты, реализуемые межсетевым экраном (МЭ): фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам (наиболее распространённым); управление списками доступа на маршрутизаторах. Типы МЭ. Пакетные фильтры. Шлюзы уровня соединения. Шлюзы прикладного уровня. Технологии Proxy и Stateful inspection. Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей. Два вида средств поддержания высокой доступности: обеспечение отказоустойчивости (нейтрализация отказов, живучесть) и обеспечение безопасного и быстрого восстановления после отказов (обслуживаемость).	Знает: основные понятия экранирования и туннелирования; типы межсетевых экранов; функции и компоненты виртуальных частных сетей VPN. Умеет: использовать межсетевые экраны для обеспечения безопасности межсетевого взаимодействия. Владеет: методикой и стандартами построения защищённых виртуальных частных сетей VPN.
9.	**Защита компьютерных систем от вирусов и вредоносных программ**	Классификация компьютерных вирусов и вредоносных программ. Файловые, загрузочные и сетевые вирусы. Методы и средства борьбы с вирусами и вредоносными программами. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения. Механизмы распространения вирусов. Каналы распространения вирусов. Классические компьютерные вирусы. Макровирусы. Троянские программы. Сетевые черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.	Знает: классификацию компьютерных вирусов и вредоносных программ; методы и средства борьбы с вирусами и вредоносными программами. Умеет: обеспечивать комплексную защиту информации. Владеет: навыками антивирусной борьбы и использования антивирусного ПО.

5. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

№ п/п	№ раздела	Тема семинара	Кол-во часов
1	2	Характеристика и механизмы реализации типовых удаленных атак. Понятие типовой удаленной атаки. Анализ сетевого трафика. Подмена доверенного объекта или субъекта РВС. Ложный объект РВС. Внедрение в РВС ложного объекта путем навязывания ложного маршрута.	12

		Внедрение в РВС ложного объекта путем использования недостатков алгоритмов удаленного поиска. Использование ложного объекта для организации удаленной атаки на РВС. Селекция потока информации и сохранение ее на ложном объекте РВС. Модификация информации. Подмена информации. Отказ в обслуживании.	
2	5	Управление доступом. Матрица доступа. Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом. Основы Active Directory Domain Services. Основы работы с групповыми политиками.	4
3	6	Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA.	6
4	7	Применение аудита в ОС семейства Windows для отслеживания деятельности пользователей. Настройка политики аудита. Аудит в Windows Server 2008/2012.	2
5	8	Механизмы защиты, реализуемые межсетевым экраном (МЭ): фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам; управление списками доступа на маршрутизаторах. Типы межсетевых экранов. Пакетные фильтры. Шлюзы уровня соединения. Stateful Inspection firewall. Host-based firewall. Примеры правил. Персональные firewall и персональные устройства firewall. Шлюзы прикладного уровня. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Примеры правил. Трансляция сетевых адресов (NAT). Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей.	8
6	9	Троянские программы. Сетевые черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.	4
		Итого:	**36**

6. ЛАБОРАТОРНЫЕ РАБОТЫ

№ п/п	№ раздела	Тематика лабораторных работ	Кол-во часов
1	5	Лабораторная работа №1. Разграничение прав пользователей в защищенных версиях операционной системы Windows.	2
2	5	Лабораторная работа №2. Реализация политики безопасности в защищенных версиях операционной системы Windows.	4
3	5	Лабораторная работа №3. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.	2
4	6	Лабораторная работа №4. Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов.	4
5	7	Лабораторная работа №5. Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.	4
6	2,9	Лабораторная работа №6. Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности при использовании глобальных вычислительных сетей.	2
		Итого:	**18**

Методические указания по выполнению лабораторных работ (лабораторный практикум) выдаются студентам в электронном виде. Студентам выдаются шесть файлов, содержащих задания и всю необходимую методическую информацию.

7. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

По дисциплине не предусмотрены курсовые работы, контрольные работы, рефераты.

8. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

В результате самостоятельной работы студент должен:

- **иметь представление** об информации, способах ее представления, о задачах объектах, предмете, методах информационной безопасности; об официальных органах, обеспечивающие информационную безопасность в Российской Федерации; о правовом обеспечении информационной безопасности; о концепции информационной безопасности Российской Федерации; различиях между стеганографией и криптографией.
- **знать** структуру информации, понятие «электронный документ» и «электронная подпись»; какие опасности и угрозы, возникают при использовании информации; основные понятия и классификацию средств криптографической защиты информации; основные методы симметричного шифрования; основные методы построения асимметричных криптосистем; классификацию компьютерных вирусов и вредоносных программ; методы и средства борьбы с вирусами и вредоносными программами.
- **уметь** использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; использовать алгоритмы генерации, хранения и распределения ключей; использовать антивирусное программное обеспечение.

Студенты выполняют задания, самостоятельно обращаясь к учебной литературе. Проверка выполнения заданий осуществляется путем электронного тестирования и устного опроса на практических занятиях. Для методического обеспечения самостоятельной работы студентов разработан информационный комплекс из трех частей, охватывающий все темы курса, вынесенные на самостоятельное изучение. Информационный комплекс выдается студентам в электронном виде.

№ п/п	Наименование темы	Виды самостоятельной работы	Формы контроля
1	Политика в сфере обеспечения информационной безопасности России. Концептуальная модель информационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Федеральный закон «О государственной	изучение	тестирование

	тайне». Управление доступом. Матрица доступа. Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом. Безопасность операционной системы WINDOWS.		
2	Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Основные свойства асимметричных криптосистем. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи. Схемы неоспоримой подписи.	изучение	тестирование
3	Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения. Механизмы распространения вирусов. Каналы распространения вирусов. Классические компьютерные вирусы. Макровирусы. Троянские программы. Черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.	изучение	тестирование

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Список рекомендованной литературы

№	Название, библиографическое описание	Кол-во экз. в библ. (на каф.)
1	Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. - М.: Форум : ИНФРА-М, 2014.	1
2	Мельников В. П.Информационная безопасность и защита информации. - М.: Академия, 2008.	5
3	Информационная безопасность открытых систем. - М.: Горячая линия-Телеком, 2008.	5

Дополнительная литература

1. Леванский В.А. Моделирование в социально-правовых исследованиях. М.: Наука, 1986. 160 с.

2. Наумов В.Б. Право и Интернет: Очерки теории и практики. - М.: Книжный дом «Университет», 2002.
3. Норткатт С., Новак Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу, Москва - Лори, 2001.
4. Овчинский А.С. Информация и оперативно-розыскная деятельность. –М.: Инфра-М, 2002. 97 с.

Программное обеспечение

1. Стандартный пакет офисных программ корпорации Microsoft (Excel).
2. СПС «КонсультантПлюс».
3. Программное средство PGP (Pretty Good Privacy) —программа для шифрования информации и создания электронных цифровых подписей, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске.

Базы данных, информационно-справочные и поисковые системы

1. http://intuit.ru/
2. http://citforum.ru/
3. Электронный каталог научной библиотеки УлГУ.
4. Научная электронная библиотека eLibrary.ru.
5. Электронная библиотечная система IPRbooks.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Аудитории для проведения лекционных и семинарских занятий оснащенное проектором, ноутбуком, аудиооборудованием для просмотра видео (актовый зал, 703, 709 и др. аудитории).
2. Аудитории, оборудованные интерактивными досками (603, 611)
3. Аудитории для проведения тестирования и самостоятельной работы студентов с выходом в интернет, комп.класс №806 (корпус по ул. Пушкинская, 4а), 1 сервер и 16 рабочих мест (MS Office).
4. Читальный зал (803 аудитория) с компьютеризированными рабочими местами для работы с электронными библиотечными системами, каталогом и т.д.

Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Информационная безопасность»

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенция по дисциплине «Информационная безопасность» для студентов направления «Бизнес-информатика»

№ семестра	Дисциплины (модули)	Код компетенции		
		ОПК-1	ПК-9	
3	Деловые коммуникации	+		
3	Информационная безопасность	+	+	
4	Учебная практика	+		
8	Производственная практика	+	+	
8	Дипломная практика	+	+	
8	Государственная итоговая аттестация	+	+	

2. Компетенции, которые формируются в процессе изучения дисциплины

ОПК-1; ПК-9.

Показатели и критерии оценивания, шкала оценивания

Критерий оценивания – умение правильно отвечать на вопросы тестового задания;
Показатель оценивания – процент верных ответов на вопросы тестового задания;
Шкала оценивания – выделено четыре уровня оцениваемых компетенций:
высокий – не менее 90% правильных ответов;
достаточный - не менее 70% правильных ответов;
пороговый - не менее 40% правильных ответов;
критический - менее 40% правильных ответов.

3. Требования к результатам освоения дисциплины

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны:		
			знать	уметь	владеть
1	ОПК-1	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	– основные понятия, изложенные в Доктрине информационной безопасности РФ и Федеральном Законе «Об информации, информационных технологиях и защите информации»; интересы личности, общества и государства в информационной области; понятие ценности информации, защиты информации, системы защиты информации; цели и концептуальные основы защиты информации; основные виды угроз безопасности информации и их классификацию; – классификацию стандартов в области информационной безопасности; руководящие документы Гостехкомиссии России; направления защиты от несанкционированного доступа.	– производить анализ типов информации в зависимости от порядка ее предоставления; делать разбор методов обеспечения информационной безопасности; классифицировать в соответствии с уровнями обеспечения национальной безопасности группы субъектов; подразделять основные средства защиты по видам деятельности; пользоваться в своей профессиональной деятельности основными нормативными правовыми актами в сфере обеспечения информационной безопасности;	– методами классификации конфиденциальной информации; навыками работы с документами в сфере обеспечения информационной безопасности; – методами классификации угроз безопасности информации в распределенных вычислительных системах; – основными сетевыми командами ОС Windows, используемыми для обеспечения безопасности распределенных вычислительных систем; – методами и способами управления персоналом; организации физической защиты; поддержания работоспособности; реагирования на нарушения режима безопасности; планирования восстановительных работ.
2	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры	– понятие угроз безопасности; способы классификации угроз информационной безопасности; – технологически	– проектировать и использовать средства идентификации и аутентификации пользователей; – использовать криптографические	– идеологией произвольного (дискреционного) управления доступом, принудительного (мандатного) управления

		предприятия	е возможности злоумышленнико в по преодолению систем защиты информации; характеристики и механизмы реализации типовых удаленных атак; понятие типовой удаленной атаки; уязвимости сетевых протоколов ARP, ICMP, DNS, TCP, FTP, TELNET; принципы создания защищенных систем связи в распределенных вычислительных системах; – понятие сервиса безопасности; понятие архитектурной безопасности; назначение списков управления доступом; принципы функционировани я системы S/KEY и сервера аутентификации Kerberos	методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; использовать алгоритмы генерации, хранения и распределения ключей; – использовать методы активного аудита; – использовать межсетевые экраны для обеспечения безопасности межсетевого взаимодействия; – обеспечивать комплексную защиту информации.	доступом, ролевого управления доступом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет; – инструментами ОС семейства Windows для настройка политики аудита; – методикой и стандартами построения защищённых виртуальных частных сетей VPN; – навыками антивирусной борьбы и использования антивирусного ПО.

4. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства		Технология оценки (способ контроля)
			наименование	№№ заданий	
1	Введение в информационную безопасность.	ОПК-1	Вопросы к экзамену	1, 2	опрос
2	Классификация и характеристика угроз безопасности информации.	ОПК-1	Вопросы к экзамену	3	опрос
3	Стандарты и спецификации в области информационной безопасности.	ОПК-1	Вопросы к экзамену	41-43	опрос
4	Административный	ОПК-1	Вопросы к	44	опрос

	уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности.		экзамену		
5	Идентификация и аутентификация, управление доступом.	ПК-9	Вопросы к экзамену	6, 7, 32, 37	опрос
6	Методы криптографической защиты информации. Электронная цифровая подпись.	ПК-9	Вопросы к экзамену	9, 28-31, 33-36	опрос
7	Протоколирование и аудит, контроль целостности.	ПК-9	Вопросы к экзамену	8	опрос
8	Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование.	ПК-9	Вопросы к экзамену	11, 38-40	опрос
9	Защита компьютерных систем от вирусов и вредоносных программ	ПК-9	Вопросы к экзамену Тестирование	17-27, 47-50 1-20	опрос электронное тестирование

5. Оценочные средства для промежуточной аттестации

5.1. Вопросы к экзамену

Индекс компетенции	№ задания	Формулировка вопроса
ОПК-1	1	Понятие информационной безопасности
ОПК-1	2	Основные составляющие информационной безопасности
ОПК-1	3	Основные определения и критерии классификации угроз
ОПК-1	4	Классификация типовых удаленных атак
ПК-9	5	Основные понятия программно-технического уровня информационной безопасности
ПК-9	6	Сервис безопасности идентификация и аутентификация
ПК-9	7	Сервис безопасности управление доступом
ПК-9	8	Сервис безопасности протоколирование и аудит
ПК-9	9	Сервис безопасности шифрование
ПК-9	10	Сервис безопасности контроль целостности
ПК-9	11	Сервис безопасности экранирование
ПК-9	12	Сервис безопасности анализ защищенности
ПК-9	13	Сервис безопасности обеспечение отказоустойчивости
ПК-9	14	Сервис безопасности обеспечение безопасного восстановления
ПК-9	15	Сервис безопасности туннелирование
ПК-9	16	Сервис безопасности управление
ПК-9	17	Классификация вирусов
ПК-9	18	Средства антивирусной защиты
ПК-9	19	Типовая удаленная атака "Анализ сетевого трафика"
ПК-9	20	Типовая удаленная атака "Подмена доверенного объекта или субъекта распределенной вычислительной системы"
ПК-9	21	Типовая удаленная атака "Внедрение в распределенную вычислительную систему ложного объекта путем навязывания ложного маршрута"
ПК-9	22	Типовая удаленная атака "Отказ в обслуживании"

ПК-9	23	Ложный ARP-сервер в сети Internet
ПК-9	24	Ложный DNS-сервер в сети Internet
ПК-9	25	Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети Internet ложного маршрутизатора
ПК-9	26	Подмена одного из субъектов TCP-соединения в сети Internet
ПК-9	27	Причины успеха удаленных атак на распределенные вычислительные системы
ПК-9	28	Криптография
ПК-9	29	Какие цели преследует криптография? Перечислите основные алгоритмы криптографических преобразований
ПК-9	30	Перечислите основные методы криптографической защиты информации в компьютерных системах и сетях
ПК-9	31	Как классифицируются средства криптографической защиты информации?
ПК-9	32	Перечислите основные схемы идентификации пользователя
ПК-9	33	Преимущества и недостатки асимметричных криптосистем. С какой целью в асимметричных криптосистемах используются два ключа?
ПК-9	34	Как обеспечивается криптостойкость асимметричных криптосистем?
ПК-9	35	Каково основное назначение хэш-функции? Каковы основные принципы формирования хэш-функции? Какими свойствами должна обладать хэш-функция, используемая в процессе аутентификации?
ПК-9	36	Где и с какой целью используется электронная цифровая подпись? Перечислите основные этапы формирования электронной цифровой подписи. Какими свойствами должна обладать электронная цифровая подпись? Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия
ПК-9	37	Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными
ПК-9	38	Перечислите функции и компоненты сети VPN
ПК-9	39	Классифицируйте VPN по способу технической реализации и архитектуре технического решения
ПК-9	40	Каковы способы защиты информации при межсетевом взаимодействии?
ОПК-1	41	Стандарты в информационной безопасности. Понятие стандарта.
ОПК-1	42	Классификация стандартов в области информационной безопасности. "Оранжевая книга", ее структура и группы классов защищенности.
ОПК-1	43	Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"
ОПК-1	44	Административный уровень информационной безопасности. Основные понятия. Политика безопасности. Программа безопасности
ОПК-1	45	Сервисы безопасности
ПК-9	46	Классификация удаленных атак на распределенные вычислительные системы
ПК-9	47	Понятие типовой удаленной атаки
ПК-9	48	Классические вирусы
ПК-9	49	Троянские программы
ПК-9	50	Сетевые черви

Показатели и критерии оценивания, шкала оценивания

От студентов требуется обязательное посещение лекций и семинаров, выполнение комплекса лабораторных работ, участие в аттестационных испытаниях, активная работа на семинарах.

Промежуточная аттестация по итогам освоения программы учебной дисциплины в 3-ем семестре проводится в форме экзамена. Экзамен сдается согласно расписанию и служит формой проверки учебных достижений обучающихся по первой части программы учебной дисциплины и преследуют цель - оценить учебные достижения за академический период.

Положительная оценка ставится студенту:

- при полном раскрытии вопросов билета;
- при условии успешного прохождения тестирования.

предполагает:

- наличие системы знаний по предмету;
- умение излагать материал в логической последовательности, систематично, грамотным языком;
- владение специализированной терминологией;
- знание основных сервисов безопасности, способы и механизмы их реализации;
- знание государственной политики в области обеспечения информационной безопасности
- умение применять на практике методы, средства и уровни защиты информации;
- владение основными технологиями информационной безопасности и умение применять их в профессиональной деятельности.

Шкала оценивания:

- оценка «отлично» выставляется, если даны правильные и четкие ответы на вопросы билета, правильные и четкие ответы на дополнительные вопросы, продемонстрирована способность формировать и обоснованно отстаивать собственное мнение;
- оценка «хорошо» выставляется, если даны правильные, но не всегда полные ответы на вопросы билета, дополнительные вопросы; возникают трудности в формировании обоснованного собственного мнения;
- оценка «удовлетворительно» выставляется, если даны правильные, но не полные ответы на вопросы билета, возникают проблемы при ответе на дополнительные вопросы, проблемы при формировании собственного мнения;
- оценка «неудовлетворительно» выставляется, если ответы на основные вопросы даны в объеме менее 50%, ответы на дополнительные вопросы вызывают большие затруднения (практически не верны).

5.2. Примерные тестовые задания

Индекс компетенции	№ задания	Формулировка вопроса
ПК-9	1	Какие вирусы практически исчезли после массового перехода на операционные системы семейства Windows Загрузочные вирусы Файлово-загрузочные вирусы Файловые вирусы Макровирусы Скрипт-вирусы
ПК-9	2	Первая реализация вируса появилась в период конец 60-х гг. конец 70-х гг. конец 80-х гг. конец 50-х гг.
ПК-9	3	Первый сетевой вирус Creeper появился в начале 70-х гг. в начале 80-х гг. в конце 70-х гг. в середине 60-х гг. в середине 80-х гг.
ПК-9	4	BOMBSQAD - это антивирусная программа червь троянская программа загрузочный вирус

		файловый вирус
ПК-9	5	Какой из известных программистов заявлял, что вирусов не существует и сравнивал их со сказками о крокодилах, живущих в канализации Нью-Йорка? Питер Нортон Джеки Чан Джон фон Нейман Анди Хопкинс Билл Гейтс Роберт Моррис
ПК-9	6	Какая организация создана специально для борьбы с вредоносным ПО? CERT ISO CERN ISOC IEEE
ПК-9	7	Первая эпидемия троянской программы была вызвана Aids Information Diskette Suriv Virdem Cascade
ПК-9	8	Первый полиморфный вирус - это Chameleon Voronezh Cascade Datacrime
ПК-9	9	Вирусов, заражающий исходные тексты программ (C и Pascal) SrcVir Dir_II Shifter OneHalf
ПК-9	10	Первый макровирус, поражавший документы Microsoft Word, - это Concept Form Win.Vir Chameleon
ПК-9	11	Способы размножения вируса: машинозависимый машиннонезависимый косвенный системный
ПК-9	12	Укажите способы размножения вируса: полиморфный олигоморфный машинозависимый комплексный
ПК-9	13	Сигнатурным методом можно обнаружить обычные, неполиморфные вирусы олигоморфные вирусы полиморфные вирусы
ПК-9	14	В основе сигнатурного метода лежит обнаружение вируса по строке его кода обнаружение вируса по способу размножения обнаружение вируса по факту изменения размера файла обнаружение вируса по характерному для зловредного ПО поведению
ПК-9	15	Для троянской программы характерно троян способен только к выполнению вредоносных функций и не может размножаться троян способен только к выполнению вредоносных функций и может

		размножаться троян не способен к выполнению вредоносных функций и может размножаться троян не способен к выполнению вредоносных функций и не может размножаться
ПК-9	16	Процесс размножения компьютерного вируса может быть условно разделен на следующие стадии Проникновение на компьютер Активация вируса Поиск объектов для заражения Подготовка вирусных копий Внедрение вирусных копий
ПК-9	17	Вирус, который записывает свой код в MBR жесткого диска, относится к категории Загрузочные вирусы Файловые вирусы Макровирусы Скрипт-вирусы
ПК-9	18	Резидентность - способность вируса сохранять активность после того, как зараженная программа закончила свою работу способность вируса скрывать свое присутствие на компьютере способность вируса внедряться в служебные программы операционной системы способность вируса получать в системе наивысший приоритет
ПК-9	19	Какие вирусы практически исчезли после массового перехода на операционные системы семейства Windows Загрузочные вирусы Файлово-загрузочные вирусы Файловые вирусы Макровирусы Скрипт-вирусы
ПК-9	20	Зловредные программы - Модификаторы настроек браузера - относятся к категории Троянов Червей Файловых вирусов Макровирусов

Показатели и критерии оценивания, шкала оценивания

При прохождении теста учитывается время прохождения теста (20 заданий – 20 минут) и количество правильных ответов.

Шкалы оценок:

- оценка «неудовлетворительно» - при условии правильного ответа менее чем на 40% тестовых заданий;
- оценка «удовлетворительно» - при условии правильного ответа не менее чем на 40% тестовых заданий;
- оценка «хорошо» - при условии правильного ответа не менее чем на 70% тестовых заданий;
- оценка «отлично» - при условии правильного ответа не менее чем на 90% тестовых заданий.