Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Алмосов Александр Павлович

Подписан: Алмосов Александр Павлович
DN: C=RU, L=Волгоград, O=ВИУ РАНХиГС, OU=Директорат, CN=Алмосов Александр Павлович, E=almosov-ap@ranepa.ru
Основание: я подтверждаю этот документ
Местоположение: ВИУ - филиал РАНХиГС
Дата: 2020.12.10 14:20:11+04'00'
Foxit Reader Версия: 10.1.1

Волгоградский институт управления – филиал РАНХиГС

Экономический факультет
Кафедра информационных систем и математического моделирования

УТВЕРЖДЕНА

решением кафедры

информационных систем и математического моделирования

Протокол от «28» августа 2017 г. № 1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.3.2 ПРАВОВАЯ ИНФОРМАТИКА

(индекс и наименование дисциплины, в соответствии с учебным планом)

38.05.01 Экономическая безопасность

(код и наименование направления подготовки (специальности))

"Экономико-правовое обеспечение экономической безопасности"

направленность (профиль/специализация)

Экономист

квалификация

Очная, заочная

форма(ы) обучения

Год набора – 2018 г.

Волгоград, 2017 г.

Автор(ы)-составитель(и):

канд. техн. наук,
доцент кафедры информационных систем
и математического моделирования И.П. Михнев

Заведующий кафедрой информационных
систем и математического моделирования О.А. Астафурова

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Дисциплина **Б1.В.ДВ.3.2 Правовая информатика** обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	Способность применять проектный подход при решении профессиональных задач	УК ОС-2.4.2	Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью обеспечения информационной безопасности

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ[1] *(при наличии профстандарта)*/ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
УК ОС-2 направлена на формирование глубоких знаний в области информационных технологий, необходимых для приобретения навыков и умений управления информацией, как взаимосвязанной и соответствующим образом сформированной совокупности: организационных, управленческих, экономических, информационных, методических, программно-технологических аспектов деятельности по удовлетворению информационных потребностей с целью принятия эффективного решения, и по наращиванию интеллектуального потенциала в виде информационных баз данных и баз знаний.	УК ОС-2.4.2	На уровне знаний: Сформулировать базовые теоретические представления о правовой информации, процессах оборота информации и информатизации в правовой сфере; определить средства, методы и технологии решения профессионально-ориентированных задач с применением новейших компьютерных и коммуникационных технологий; назвать основные методы обеспечения информационной безопасности; дать определение основных положений теории информационной безопасности информационных систем; характеризовать модели безопасности и их применение; назвать способы нарушений информационной безопасности.
		На уровне умений: Определить опасности и угрозы информационной безопасности; применять основные методы и программы защиты информации; использовать методы и способы обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты служебной информации; применять новые информационные и телекоммуникационные технологии правовой информатики.
		На уровне навыков: Демонстрировать навыки криптографической и стеганографической защиты информации; применять основные методы и средствами защиты информации; демонстрировать навыками работы с нормативными документами по защите информации и организацией соответствующих отделов в организациях; осуществлять самостоятельное решение задач предметной области на персональном компьютере с помощью новых информационных технологий и современных информационных систем

[1] Для образовательных программ, реализуемых по ФГОС, и для универсальных компетенций первая колонка может не заполняться

2. Объем и место дисциплины в структуре ОП ВО

Учебная дисциплина Б1.В.ДВ.3.2 «Правовая информатика» относится к дисциплинам по выбору вариативной части учебного плана. Дисциплина общим объемом 72 часа (2 ЗЕ) изучается в течение одного семестра и заканчивается зачетом. На очной форме обучения дисциплина изучается в 4 семестре, на заочной форме – на 2 курсе.

Для успешного овладения дисциплиной студенту необходимо использовать знания и навыки, полученные им при изучении таких дисциплин, как математика, физика, логика.

Знания, полученные в ходе изучения дисциплины «Правовая информатика в компьютерных технологиях» могут быть полезны при изучении таких профессиональных дисциплин, как Б1.Б.9 Экономическая теория, Б1.Б.23 Экономическая безопасность, Б1.Б.30 Обеспечение защиты государственной и коммерческой тайны.

По очной форме обучения количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) – 54 часа (лекций – 20 часов, практических занятий – 34 часа), на самостоятельную работу обучающихся – 18 часов.

По заочной форме обучения количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) – 10 часов (лекций – 2 часов, практических занятий – 8 часов), на самостоятельную работу обучающихся – 58 часов, на контроль – 4 часов.

В соответствии с учебным планом формой промежуточной аттестации является зачет.

3. Содержание и структура дисциплины

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	КСР		
Очная форма обучения								
4 семестр								
Тема 1	Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и информационной безопасности.	8	2	-	4		2	*О*
Тема 2	Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	8	2	-	4		2	*О*
Тема 3	Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации	8	2	-	4		2	*О*

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	КСР		
	по обеспечению информационной безопасности.							
Тема 4	Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	8	2	-	4		2	*О*
Тема 5	Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	10	4	-	4		2	*О*
Тема 6	Интернет в юридической деятельности. Основные технологии построения защищенных ИС. Межсетевые экраны.	8	2	-	4		2	*О*
Тема 7	Технология VPN-сетей.	8	2	-	4		2	*О*
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	8	2	-	4		2	*О*
Тема 9	Типовая структура защиты от НСД. Управление доступом.	6	2	-	2		2	*О, Т*
Промежуточная аттестация								За
Всего:		**72**	**20**		**34**		**18**	
Заочная форма обучения								
Тема 1	Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и информационной безопасности.	6,25	0,25	-	-		6	*О*
Тема 2	Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	7,25	0,25	-	1		6	*О*

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	КСР		
Тема 3	Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	7,25	0,25	-	1		6	*О*
Тема 4	Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	7,25	0,25	-	1		6	*О*
Тема 5	Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	12,25	0,25	-	4		8	*О*
Тема 6	Интернет в юридической деятельности. Основные технологии построения защищенных ИС. Межсетевые экраны.	7,25	0,25	-	1		6	*О*
Тема 7	Технология VPN-сетей.	6	-	-	-		6	*О*
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	8,25	0,25	-	-		8	*О*
Тема 9	Типовая структура защиты от НСД. Управление доступом.	6,25	0,25	-	-		6	*О, Т*
Промежуточная аттестация		4						За
Всего:		**72**	**2**		**8**		**58**	**4**

Примечание: 4 – формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э), реферат (Р), диспут (Д), задания (З) и др.

Содержание дисциплины

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Тема 1	Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и информационной безопасности.	Понятие информации, защиты информации и информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне региона и на локальном уровне. Основные положения теории информационной безопасности информационных систем. Основные составляющие обеспечения информационной безопасности хозяйственной деятельности.
Тема 2	Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	Важность законодательного уровня информационной безопасности. Обзор российского законодательства в области обеспечения информационной безопасности. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации». Другие законы и законодательные акты. Концепция информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации, нормативно-справочные документы. Нормативные акты администрации Волгограда в области информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений. Уголовная и административная ответственность.
Тема 3	Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	Понятие атаки на информационную систему. Классификация атак. Виды противников или “нарушителей”, их классификация. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально-вещественный. Понятие угрозы. Источники угроз и их классификация. Построение модели угроз организации. Примеры. Руководящие документы Гостехкомиссии России (Федеральная служба по техническому и экспортному контролю) по защите от несанкционированного доступа к информации. Специальные требования и рекомендации. Инструкция СТР-К. Рекомендации по защите конфиденциальной информации. Классы защищенности средств вычислительной техники и автоматизированных систем по руководящим документам Гостехкомиссии России. Показатели защищенности. Система защиты информации от несанкционированного доступа. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы. Разрешительная система допуска. Рекомендации по плану доработки объектов информатизации на соответствие требованиям руководящих документов Гостехкомиссии России.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Тема 4	Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	Историческая справка. Возможные направления решения задачи обеспечения передачи секретной информации. Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа. Надежность криптосистемы. Два основных направления в современной криптографии. Классические криптосистемы. Одноалфавитные и многоалфавитные криптосистемы. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера. Надежность многоалфавитных систем. Электромеханические шифровальные машины. Абсолютно надежная криптосистема: “Одноразовый блокнот”. Возможность использования таких систем на практике. Стандарты шифрования данных. Криптосистема DES. Российский стандарт шифрования ГОСТ 28147-89. Проблема выбора надежной криптосистемы для защиты своих данных. Перспективы развития криптоанализа. Проблема полного перебора всех ключей.
Тема 5	Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	Системы шифрования, не требующие передачи ключа. Проблемы использования таких систем. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом. Понятие открытого и секретного ключа. Правила их использования. Принципы построения криптосистем с открытым ключом. Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA. Длина ключа в криптографии с открытым ключом. Односторонняя функция, возможность ее использования. Электронная подпись и принципы ее применения.
Тема 6	Интернет в юридической деятельности. Основные технологии построения защищенных ИС. Межсетевые экраны.	Основные технологии построения защищенных ИС. Понятие межсетевого экрана. Правила фильтрации и принципы их применения. Пакетные фильтры. Политика сетевой безопасности. Политика реализации межсетевых экранов. Функциональные требования к межсетевым экранам и их компоненты. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров. Схемы организации межсетевых экранов. Особенности различных схем реализации, их преимущества и недостатки. Проблемы, связанные с межсетевыми экранами. Требования к межсетевым экранам

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Тема 7	Технология VPN-сетей.	Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей. Особенности VPN. Туннель VPN. Туннелирование и его особенности. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN. Угрозы для VPN. Варианты защищенных соединений. Классификация VPN-сетей. Совмещение VPN-технологий и межсетевого экрана. Недостатки VPN.
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе с Интернет. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.
Тема 9	Типовая структура защиты от НСД. Управление доступом.	Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация. Парольная аутентификация. Правила применения паролей. Одноразовые пароли. Сервер аутентификации. Подсистема управления доступом, подсистема регистрации и учета. Принципы контроля доступа. Матрица доступа и списки доступа. Произвольное и принудительное управление доступом. Ограничивающий интерфейс. Ролевое управление доступом. Статическое и динамическое распределение ролей. Подсистема обеспечения целостности. Криптографическая подсистема. Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентификационных признаков. Классификация устройств ввода идентификационных признаков. Биометрические устройства ввода идентификационных признаков и их классификация. Преимущества и недостатки их использования. Комбинированные устройства. Электронные замки.

На самостоятельную работу студентов по дисциплине Б1.В.ДВ.3.2 «Правовая информатика» выносятся следующие темы:

№ п/п	Тема	Вопросы, выносимые на СРС	Очная форма	Заочная форма
1	*2*	*3*	*4*	*5*
1.	Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и	Понятие информации, защиты информации и информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне региона и на локальном уровне. Основные положения теории информационной безопасности информационных	*О*	*О*

	информационной безопасности.	систем.		
2.	Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	Обзор российского законодательства в области обеспечения информационной безопасности. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации». Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации. Нормативные акты администрации Волгограда в области информационной безопасности.	*О*	*О*
3.	Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	Понятие атаки на информационную систему. Классификация атак. Виды противников или “нарушителей”, их классификация. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально-вещественный. Понятие угрозы. Источники угроз и их классификация. Построение модели угроз организации. Примеры. Специальные требования и рекомендации. Показатели защищенности. Система защиты информации от несанкционированного доступа. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы. Разрешительная система допуска.	*О*	*О*
4.	Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа. Надежность криптосистемы. Два основных направления в современной криптографии. Одноалфавитные и многоалфавитные криптосистемы. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера. Надежность многоалфавитных систем. Абсолютно надежная криптосистема: “Одноразовый блокнот”. Криптосистема DES.	*О*	*О*
5	Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	Системы шифрования, не требующие передачи ключа. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом. Понятие открытого и секретного ключа. Принципы построения криптосистем с открытым ключом. Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA. Длина ключа в криптографии с открытым ключом. Односторонняя функция, возможность ее использования. Электронная подпись и принципы ее применения.	*О*	*О*
6	Интернет в юридической деятельности. Основные технологии построения	Основные технологии построения защищенных ИС. Понятие межсетевого экрана. Правила фильтрации и принципы их применения. Пакетные фильтры. Политика сетевой безопасности. Политика реализации межсетевых экранов. Функциональные	*О*	*О*

	защищенных ИС. Межсетевые экраны.	требования к межсетевым экранам и их компоненты. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров. Схемы организации межсетевых экранов. Требования к межсетевым экранам		
7	Технология VPN-сетей.	Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей. Особенности VPN. Туннелирование и его особенности. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN. Угрозы для VPN. Классификация VPN-сетей. Совмещение VPN-технологий и межсетевого экрана. Недостатки VPN.	*О*	*О*
8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе с Интернет. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.	*О*	*О*
9	Типовая структура защиты от НСД. Управление доступом.	Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация. Парольная аутентификация. Правила применения паролей. Одноразовые пароли. Принципы контроля доступа. Матрица доступа и списки доступа. Произвольное и принудительное управление доступом. Ограничивающий интерфейс. Ролевое управление доступом. Криптографическая подсистема. Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентиф-ных признаков. Преимущества и недостатки их использования. Электронные замки.	*О, Т*	*О, Т*

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств по дисциплине

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.ДВ.3.2 «Правовая информатика» используются следующие формы и методы текущего контроля успеваемости обучающихся:

№ п/п	Наименование тем (разделов)	Методы текущего контроля успеваемости
Очная форма		
Тема 1	Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и информационной безопасности.	Устный опрос
Тема 2	Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за	Устный опрос

	совершение компьютерных преступлений.	
Тема 3	Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	Устный опрос
Тема 4	Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	Устный опрос
Тема 5	Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	Устный опрос
Тема 6	Интернет в юридической деятельности. Основные технологии построения защищенных ИС. Межсетевые экраны.	Устный опрос
Тема 7	Технология VPN-сетей.	Устный опрос
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Устный опрос
Тема 9	Типовая структура защиты от НСД. Управление доступом.	Устный опрос, тестирование
Заочная форма		
Тема 1	Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и информационной безопасности.	Устный опрос
Тема 2	Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	Устный опрос
Тема 3	Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	Устный опрос
Тема 4	Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	Устный опрос
Тема 5	Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	Устный опрос
Тема 6	Интернет в юридической деятельности. Основные технологии построения защищенных ИС. Межсетевые экраны.	Устный опрос
Тема 7	Технология VPN-сетей.	Устный опрос
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Устный опрос
Тема 9	Типовая структура защиты от НСД. Управление доступом.	Устный опрос, тестирование

4.1.2. Промежуточная аттестация проводится в форме зачета методом устного опроса и выполнения заданий на компьютере.

К сдаче зачета по дисциплине допускаются студенты, получившие не меньше 60 баллов при текущей аттестации. При подготовке к зачету студент внимательно просматривает вопросы, предусмотренные рабочей программой, и знакомиться с рекомендованной основной литературой. Основой для сдачи зачета студентом является изучение конспектов обзорных лекций, прослушанных в течение семестра, информация, полученная в результате самостоятельной работы, и практические навыки, освоенные при решении задач в течение семестра.

4.2. Материалы текущего контроля успеваемости.

Тема 1

Информационное общество и право. Предмет и методы правовой информатики. Понятие информации, защиты информации и информационной безопасности.

Вопросы устного опроса:

1. Понятие информации, защиты информации и информационной безопасности.
2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне региона и на локальном уровне.
3. Основные положения теории информационной безопасности информационных систем.
4. Основные составляющие обеспечения информационной безопасности хозяйственной деятельности.

Тема 2

Государственная информационная политика. Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.

Вопросы устного опроса:

1. Важность законодательного уровня информационной безопасности.
2. Обзор российского законодательства в области обеспечения информационной безопасности.
3. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации».
4. Другие законы и законодательные акты. Концепция информационной безопасности.
5. Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации, нормативно-справочные документы. Нормативные акты администрации Волгограда в области информационной безопасности.
6. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.
7. Уголовная и административная ответственность.

Тема 3

Технология работы в справочно-правовых системах. Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информ. безопасности.

Вопросы устного опроса:

1. Понятие атаки на информационную систему.
2. Классификация атак. Виды противников или “нарушителей”, их классификация.
3. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально-вещественный.
4. Понятие угрозы. Источники угроз и их классификация.
5. Построение модели угроз организации. Примеры.
6. Руководящие документы Гостехкомиссии России (Федеральная служба по техническому и экспортному контролю) по защите от несанкционированного доступа к информации. Специальные требования и рекомендации. Инструкция СТР-К.
7. Рекомендации по защите конфиденциальной информации. Классы защищенности средств вычислительной техники и автоматизированных систем по руководящим документам Гостехкомиссии России.
8. Показатели защищенности. Система защиты информации от несанкционированного доступа.
9. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы.
10. Разрешительная система допуска. Рекомендации по плану доработки объектов информатизации на соответствие требованиям руководящих документов Гостехкомиссии России.

Тема 4

Информационная безопасность. Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.

Вопросы устного опроса:

1. Историческая справка. Возможные направления решения задачи обеспечения передачи секретной информации.
2. Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации.
3. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа.
4. Надежность криптосистемы. Два основных направления в современной криптографии. Классические криптосистемы.
5. Одноалфавитные и многоалфавитные криптосистемы.
6. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера.
7. Надежность многоалфавитных систем. Электромеханические шифровальные машины.
8. Абсолютно надежная криптосистема: “Одноразовый блокнот”. Возможность использования таких систем на практике. Стандарты шифрования данных.
9. Криптосистема DES. Российский стандарт шифрования ГОСТ 28147-89. Проблема выбора надежной криптосистемы для защиты своих данных.
10. Перспективы развития криптоанализа. Проблема полного перебора всех ключей.

Тема 5

Электронный документооборот и электронная подпись. Криптография с открытым ключом. Системы шифрования. Электронная подпись.

Вопросы устного опроса:

1. Системы шифрования, не требующие передачи ключа.
2. Проблемы использования таких систем. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом.
3. Понятие открытого и секретного ключа. Правила их использования.
4. Принципы построения криптосистем с открытым ключом.
5. Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA.
6. Длина ключа в криптографии с открытым ключом.
7. Односторонняя функция, возможность ее использования.
8. Электронная подпись и принципы ее применения.

Тема 6

Интернет в юридической деятельности. Основные технологии построения защищенных ИС. Межсетевые экраны.

Вопросы устного опроса:

1. Основные технологии построения защищенных ИС.
2. Понятие межсетевого экрана. Правила фильтрации и принципы их применения. Пакетные фильтры. Политика сетевой безопасности.
3. Политика реализации межсетевых экранов. Функциональные требования к межсетевым экранам и их компоненты.
4. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров.
5. Схемы организации межсетевых экранов. Особенности различных схем реализации, их преимущества и недостатки.
6. Проблемы, связанные с межсетевыми экранами.
7. Требования к межсетевым экранам

Тема 7

Технология VPN-сетей.

Вопросы устного опроса:

1. Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей.
2. Особенности VPN. Туннель VPN. Туннелирование и его особенности.
3. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN.
4. Угрозы для VPN. Варианты защищенных соединений.
5. Классификация VPN-сетей. Совмещение VPN-технологий и межсетевого экрана. Недостатки VPN.

Тема 8

Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.

Вопросы устного опроса:

1. Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет.
2. Информационная безопасность в условиях функционирования в России глобальных сетей.
3. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет.
4. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе с Интернет.
5. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.

Тема 9

Типовая структура защиты от НСД. Управление доступом.

Вопросы устного опроса:

1. Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация.
2. Парольная аутентификация. Правила применения паролей.
3. Одноразовые пароли. Сервер аутентификации. Подсистема управления доступом, подсистема регистрации и учета.
4. Принципы контроля доступа. Матрица доступа и списки доступа.
5. Произвольное и принудительное управление доступом. Ограничивающий интерфейс.
6. Ролевое управление доступом. Статическое и динамическое распределение ролей. Подсистема обеспечения целостности. Криптографическая подсистема.
7. Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентификационных признаков. Классификация устройств ввода идентификационных признаков. Биометрические устройства ввода идентификационных признаков и их классификация.
8. Преимущества и недостатки их использования. Комбинированные устройства. Электронные замки.

ИТОГОВЫЙ ТЕСТ ПО КУРСУ
«Правовая информатика»

Электронный тест представляет собой задания с выбором только одного правильного ответа из предложенных. Результат программа Unitest выводит в процентах.

1. Правовая информатика – это…
A) общественная наука, изучающая проблемы сбора, восприятия, регистрации, хранения, обработки и использования информации, информационные процессы и технологии с использованием современных средств и методов ее автоматизированной обработки и передачи.
B) общественная наука, изучающая отрасль информационного права и использование информационных технологий.
C) наука, изучающая совокупность правовых норм и регулируемые ими общественные отношения, возникающие в процессы сбора, обработки, накопления, хранения, поиска и распространения информации.
D) прикладная наука, изучающая проблемы сбора, восприятия, регистрации, хранения, обработки и использования правовой информации
E) прикладная наука, изучающая проблемы сбора, восприятия, регистрации, хранения, обработки и использования социально-правовой информации, информационные процессы и технологии в правовой системе общества с применением современных средств и методов ее автоматизированной обработки и передачи.

2. Причины появления правовой информатики…
A) необходимость оптимизации информационных потоков в сфере правового регулирования.
B) появление ЭВМ, распространение информационно-коммуникационных технологий.
C) усложнения правового регулирования общественных процессов и необходимость повышения эффективности деятельности юристов.
D) необходимость автоматизации обработки статистической информации.
E) необходимость разработки методов и средств борьбы с компьютерной преступностью.

3. К основным направлениям развития правовой информатики относится
A) разработка автоматизированных систем для государственных органов
B) организация учета нормативных актов
C) систематизация российского законодательства
D) автоматизация обработки правовой информации
E) применение вычислительной техники в подготовке юридических кадров

4. Информационная сфера подразделяется на следующие предметные области
A) создание и распространение исходной и производной информации
B) формирование информационных ресурсов
C) реализация права на поиск, получение, передачу и потребление информации
D) создание и применение информационных систем и технологий
E) создание и применение средств и механизмов информационной безопасности

5. Из чего состоит единое информационное пространство
A) средства информационного взаимодействия граждан и организаций
B) информационные ресурсы, содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации
C) средства информационной безопасности
D) организационные структуры, обеспечивающие функционирование пространства
E) система правовой защиты информации

6. В информатизацию общественной сферы входит:
A) защита средств массовой информации
B) формирование информационных ресурсов в негосударственном секторе
C) стимулирование деятельности потребителей информации
D) информационная поддержка предпринимательства
E) функционирование Интернет

7. Информационное право – это…
A) отрасль российского права, относящаяся к информации
B) совокупность правовых норм, регулирующих вопросы информации
C) отрасль российского права, регулирующая информационные процессы и технологии
D) совокупность правовых норм, регулирующих общественные отношения, возникающие в процессы сбора, обработки, накопления, хранения, поиска и распространения информации, когда информация является конечной целью правоотношений
E) совокупность правовых норм, регулирующих процессы сбора, обработки, накопления, хранения, поиска и распространения информации

8. Что составляет предмет информационного права
A) совокупность правовых норм, регулирующих вопросы информации
B) информация
C) информационные ресурсы
D) общественные отношения в сфере обращения информации
E) защита информации

9. Отдельные документы и массивы документов в информационных системах это:
A) базы данных
B) информационные массивы
C) электронные документы
D) информационные ресурсы
E) система документации

10. Следующие институты входят в систему информационного права
A) Управление в сфере информации и информатизации
B) Информационные ресурсы. Пользование информационными ресурсами
C) Документирование информации
D) Средства массовой информации
E) Реклама

11. Криптография это…
A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
B) наука о методах и способах раскрытия шифров
C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
E) наука о методах создания цифровой подписи

12. Какая из следующих криптоаналитических атак считается наиболее опасной?
A) при наличии только одного зашифрованного фрагмента
B) при наличии большого набора зашифрованных фрагментов

C) при наличии фрагмента открытого текста и соответствующего ему криптотекста
D) при известном методе шифрования
E) при возможности выбора любого открытого текста и получении соответствующего ему криптотекста

13. Сколько различных ключей в системе Цезаря при использовании полного русского алфавита?
A) 16 D) 256
B) 33 E) 1024
C) 66

14. Что является ключом в криптосистеме Виженера?
A) любое дробное число
B) величина сдвига исходного алфавита
C) переставленный алфавит
D) случайная последовательность букв, равная длине сообщения
E) любое слово

15. Какая из перечисленных криптосистем является системой с открытым ключом?
A) DES D) ГОСТ 28147
B) RSA E) Цезаря
C) Энигма

16. Можно ли в программе PGP воспользоваться чужим открытым ключом для расшифрования информации.
A) да
B) нет
C) да, если известен тот пароль
D) да, если пользователь даст права на расшифровку его информации и сообщит свой пароль
E) да, если перебрать все ключи

17. Как раскрываются криптосистемы одноалфавитной замены?
A) такие системы раскрыть нельзя
B) полный перебор ключей
C) анализ частот встречаемых букв
D) перебор сообщений
E) перестановки букв криптотекста

18. Криптоанализ это
A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
B) наука о методах и способах раскрытия шифров
C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
E) наука о методах создания цифровой подписи

19. Что является ключом в криптосистеме Цезаря?
A) любое слово
B) любое число

C) величина сдвига исходного алфавита
D) переставленный алфавит
E) случайная последовательность символов

20. Какова длина ключа в стандарте шифрования ГОСТ 28147?
A) 256 бит D) 1024 бит
B) 64 бит E) 2048 бит
C) 56 бит

21. На сложности решения какой математической задачи основана система RSA?
A) коды исправляющие ошибки
B) дискретный логарифм
C) задача “о рюкзаке”
D) разложение больших чисел на простые множители
E) сложение по модулю два

22. Криптографический протокол это
A) метод шифрования данных
B) метод криптоанализа данных
C) метод перехвата данных
D) алгоритм обмена информацией между различными участниками при секртеной передаче данных
E) особая криптосистема

23. Криптосистема «Одноразовый блокнот» это:
A) перестановочная система
B) одноалфавитная система простой замены
C) многоалфавитная система
D) система с открытым ключом
E) такой системы не существует

24. Какой пароль наиболее надежен?
A) Фамилия пользователя
B) Фраза из книги
C) случайная последовательность цифр
D) случайная последовательность букв
E) случайная последовательность произвольных символов

25. Какова длина ключа в системе шифрования DES?
A) 256 бит D) 1024 бит
B) 64 бит E) 512 бит
C) 2048 бит

26. Криптотекст это
A) текст исходного сообщения
B) текст зашифрованного сообщения
C) пароль
D) текст, полученный при криптоанализе
E) ключ

27. Тайнопись (стеганография) это

A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц

B) наука о методах и способах раскрытия шифров

C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией

D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата

E) наука о методах создания цифровой подписи

28. Что позволяет определить метод Казиски при криптоанализе системы Виженера?

A) пароль

B) открытый текст

C) метод шифрования

D) длину пароля

E) длину открытого текста

29. Какая криптосистема обеспечивает абсолютную надежность защиты при правильном ее использовании?

A) DES D) Одноразовый блокнот

B) RSA E) Виженера

C) ГОСТ 28147

30. Обеспечивает ли пароль на вход в Windows надежную защиту компьютера?

A) да

B) нет

C) при длине пароля более 10 символов

D) при случайном пароле

E) при регулярной смене пароля

Шкала оценивания

Устный опрос

Уровень знаний, умений и навыков обучающегося при устном ответе во время текущего контроля определяется оценками «Отлично»/ «Хорошо»/ «Удовлетворительно»/ «Неудовлетворительно».

В Волгоградском институте управления – филиале РАНХиГС принята следующая шкала соответствия рейтинговых оценок пятибалльным оценкам:

- 90 – 100% – «отлично» (5);
-75 – 89% – «хорошо» (4);
- 60 – 74 – «удовлетворительно» (3);
- менее 60% – «неудовлетворительно» (2).

Уровень знаний, умений и навыков обучающегося при устном ответе во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания при проведении устного опроса является демонстрация основных теоретических положений, в рамках осваиваемой компетенции, умение применять полученные знания на практике, овладение навыками анализа и систематизации информации.

При оценивании результатов устного опроса используется следующая шкала оценок:

100% – 95%	студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы, разъяснять их в логической последовательности;
94% – 90%	студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы, разъяснять их в логической последовательности, но допускает отдельные неточности;
89% – 85%	студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы, разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера;
84% – 80%	студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы;
79% – 75%	студент отвечает в основном правильно, но чувствуется механическое заучивание материала;
74% – 70%	в ответе студента имеются существенные недостатки, материал охвачен неполно, в рассуждениях допускаются ошибки;
69% – 65%	ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки;
64% – 60%	студент имеет общее представление о теме, но не умеет логически обосновать свои мысли;
Менее 60%	студент имеет лишь частичное представление о теме.

Тестирование

Уровень знаний, умений и навыков обучающегося при устном ответе во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критерием оценивания при проведении тестирования, является количество верных ответов, которые дал студент на вопросы теста. При расчете количества баллов, полученных студентом по итогам тестирования, используется следующая формула:

$$Б = \frac{В}{О} \times 100\%,$$

где

Б – количество баллов, полученных студентом по итогам тестирования;

В – количество верных ответов, данных студентом на вопросы теста;

О – общее количество вопросов в тесте.

Проверка реферата

Уровень знаний, умений и навыков обучающегося при проверке реферата во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания при проверке реферата является демонстрация основных теоретических положений, в рамках осваиваемой компетенции.

При оценивании результатов устного опроса используется следующая шкала оценок:

100% - 90%	Учащийся демонстрирует совершенное знание основных теоретических положений, в рамках осваиваемой компетенции.
89% - 75%	Учащийся демонстрирует знание большей части основных теоретических положений, в рамках осваиваемой компетенции.
74% - 60%	Учащийся демонстрирует достаточное знание основных теоретических положений, в рамках осваиваемой компетенции.
менее 60%	Учащийся демонстрирует отсутствие знания основных теоретических положений, в рамках осваиваемой компетенции.

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	Способность применять проектный подход при решении профессиональных задач	УК ОС-2.4.2	Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью обеспечения информационной безопасности

Описание показателей и критериев оценивания компетенции на различных этапах ее формирования

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
УК ОС-2.4.2 Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью обеспечения информационной безопасности	Сформулировать базовые теоретические представления о правовой информации, процессах оборота информации и информатизации в правовой сфере; определить средства, методы и технологии решения профессионально-ориентированных задач с применением новейших компьютерных и коммуникационных технологий; назвать основные методы обеспечения информационной безопасности; дать определение основных положений теории информационной безопасности информационных систем; характеризовать модели безопасности и их применение; назвать способы нарушений информационной безопасности.	Демонстрация знаний основных теоретических положений в полном объеме
	Определить опасности и угрозы информационной безопасности; применять основные методы и программы защиты информации; использовать методы и способы обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты служебной информации; применять новые информационные и телекоммуникационные	Умение применять знания на практике в полной мере