УТВЕРЖДАЮ:
Директор Института
экономики и управления АПК
_____ Л.И. Хоружий
“ 30 ” августа 2021 г.

Лист актуализации рабочей программы дисциплины
Б1.О.17 «Информационная безопасность»

для подготовки бакалавров
Направление: 09.03.03 «Прикладная информатика»
Направленность: «Прикладная информатика в экономике»
Форма обучения: очная

Год начала подготовки: 2019

Курс 4
Семестр 7

В рабочую программу вносятся изменения: изменяется шифр дисциплины с Б1.О.20 на Б1.О.17. Программа актуализирована для 2021 года начала подготовки.

Разработчик(и): Лемешко Т.Б., Моторин О.А., Худякова Е.В.

Рабочая программа пересмотрена и одобрена на заседании кафедры прикладной информатики, протокол № 1 от «26» августа 2021 г.

Заведующий кафедрой _____ Е.В. Худякова

Лист актуализации принят на хранение:
Заведующий выпускающей кафедрой прикладной информатики

_____ «26» 08 2021 г.

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА имени К.А. ТИМИРЯЗЕВА»
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

Институт экономики и управления АПК
Кафедра прикладной информатики

УТВЕРЖДАЮ:
Директор института
экономики и управления АПК
_____ В.В. Бутырин
«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.20 «Информационная безопасность»

для подготовки бакалавров

ФГОС ВО

Направление: 09.03.03 Прикладная информатика
Направленность: Прикладная информатика в экономике

Курс: 4
Семестр: 7

Форма обучения: очная

Год начала подготовки: 2019

Регистрационный номер _____

Москва, 2020

Разработчики: Худякова Е.В., д.э.н., профессор _____

Лемешко Т.Б., ст. преподаватель _____

«13» 01 2020 г.

Рецензент: Остапчук Т.В., к.э.н., доцент _____

«13» 01 2020 г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика и учебного плана 2019 года начала подготовки.

Программа обсуждена на заседании кафедры прикладной информатики протокол № 5 от «14» 01 2020 г.

Зав. кафедрой: Худякова Е.В., д.э.н., профессор _____

«14» 01 2020 г.

Согласовано:
Председатель учебно-методической
комиссии института экономики и управления АПК
Корольков А.Ф., к.э.н., доцент _____

«23» 01 2020 г.

Заведующий выпускающей кафедрой
прикладной информатики
Худякова Е.В., д.э.н., профессор _____

«14» 01 2020 г.

Заведующий отделом комплектования ЦНБ _____

Бумажный экземпляр РПД, копии электронных вариантов РПД и оценочных материалов получены:
Методический отдел УМУ

_____ «__» _____2020 г.

СОДЕРЖАНИЕ

Аннотация
рабочей программы учебной дисциплины
Б1.О.20 «Информационная безопасность»,
для подготовки бакалавра по направлению
09.03.03 Прикладная информатика
направленности «Прикладная информатика в экономике»

Цель освоения дисциплины: повышение уровня грамотности, информационной культуры в сфере информационной безопасности, формирование культуры личной информационной безопасности; обучение студентов принципам, методам и средствам по обеспечению информационной безопасности в профессиональной деятельности.

Место дисциплины в учебном плане: дисциплина включена в обязательную часть учебного плана по направлению подготовки 09.03.03 Прикладная информатика.

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции (индикаторы): **ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-4.3**

Краткое содержание дисциплины: Основы информационной безопасности и защиты информации. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности. Административный и процедурный уровни обеспечения информационной безопасности. Основные программно-технические меры обеспечения информационной безопасности. Информационная безопасность в профессиональной деятельности, ИТ-инфраструктуры предприятия.

Общая трудоемкость дисциплины: 144/4 (часы/зач. ед.).

Промежуточный контроль: экзамен в 7-ом семестре.

1. Цель освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является повышение уровня грамотности, информационной культуры в сфере информационной безопасности, формирование культуры личной информационной безопасности; обучение студентов принципам, методам и средствам по обеспечению информационной безопасности в профессиональной деятельности.

В результате изучения учебной дисциплины обучающиеся должны:

– знать правовые акты в области защиты информации, основные понятия и угрозы информационной безопасности, основные мероприятия по обеспечению информационной безопасности в профессиональной деятельности;

– информационно-коммуникационные технологии (ИКТ), применяемые для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;

Полученные умения должны позволить выпускнику:

– ориентироваться в программно-технических, правовых и организационных методах защиты информации;

– использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной информации или утраты защищаемой информации;

– оценивать опасность, связанную с угрозами несанкционированного доступа к информации, намеренной модификации данных и утраты служебной информации;

– использовать ИКТ, информационные ресурсы и библиографические базы данных в решении профессиональных задач, учитывать основные требования информационной безопасности при решении профессиональных задач.

При этом предполагается, что выпускник будет владеть:

– навыками безопасного использования вычислительной техники при решении профессиональных задач;

– современными общими способами обеспечения информационной безопасности;

– базовыми программно-аппаратными методами защиты информации;

– навыками применения ИКТ в научно-исследовательской работе для подготовки аннотации, научных докладов и публикаций, рефератов с учетом требований информационной безопасности;

– навыками составления технической документации, нормативно-правовых документов, стандартов на различных этапах жизненного цикла информационной системы.

2. Место дисциплины в учебном процессе

Дисциплина «Информационная безопасность» включена в обязательную часть учебного плана. Дисциплина «Информационная безопасность» реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО и Учебного плана по направлению подготовки 09.03.03 Прикладная информатика.

Предшествующими курсами, на которых непосредственно базируется дисциплина «Информационная безопасность» являются «Теоретические основы информатики», «Информационные системы и технологии», «Архитектура предприятий АПК», «Вычислительные системы, сети и телекоммуникации», «ИТ-инфраструктура организации»

Дисциплина «Информационная безопасность» является основополагающей для изучения следующих дисциплин: «Разработка распределенных систем», «Информационные системы управления производственной компанией», «Информационные системы управления взаимоотношением с клиентами»

Рабочая программа дисциплины «Информационная безопасность» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1.	**ОПК-3**	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК -3.1** Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Информационно-коммуникационные технологии (ИКТ), применяемые для решения стандартных задач профессиональной деятельности	-	-
			ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	-	Использовать ИКТ, информационные ресурсы и библиографические базы данных в решении профессиональных задач, учитывать основные требования информационной безопасности при решении профессиональных задач	-
			ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской рабо-	-	-	Навыками применения ИКТ в научно-исследовательской работе для подготовки аннотации,

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
			те с учетом требований информационной безопасности.			научных докладов и публикаций, рефератов с учетом требований информационной безопасности.
2.	**ОПК-4**	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	**ОПК-4.3** Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	-	-	Навыками составления технической документации, нормативно-правовых документов, стандартов на различных этапах жизненного цикла информационной системы

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач. единиц (144 часа), их распределение по видам работ в 7 семестре представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час.	в т.ч. по семестрам
		№ 7
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**52,4**	**52,4**
Аудиторная работа	**52,4**	**52,4**
лекции (Л)	16	16
практические занятия (ПЗ)	34	34
консультации перед экзаменом	2	2
контактная работа на промежуточном контроле (КРА)	0,4	0,4
2. Самостоятельная работа (СРС)	**91,6**	**91,6**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям и т.д.)	67	67
Подготовка к экзамену (контроль)	24,6	24,6
Вид промежуточного контроля:		Экзамен

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование тем дисциплины	Всего часов на раздел	Аудиторная Работа			Внеаудиторная работа (СРС)
		Л	ПЗ	ПКР	
Тема 1. Основы информационной безопасности и защиты информации	18	2	-	-	16
Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	37	4	10	-	23
Тема 3. Административный и процедурный уровни обеспечения информационной безопасности	22	2	-	-	20
Тема 4. Программно-технические меры обеспечения информационной безопасности	28	4	12	-	12
Тема 5. Информационная безопасность в профессиональной деятельности	36,6	4	12		20,6
Консультации перед экзаменом	2	-	-	2	-
Контактная работа на промежуточном контроле (КРА)	0,4	-	-	0,4	-
ИТОГО	**144**	**16**	**34**	**2,4**	**91,6**

Тема 1. Основы информационной безопасности и защиты информации

Актуальность проблемы обеспечения безопасности в цифровом обществе. Основные понятия и определения информационной безопасности. Основные составляющие информационной безопасности. Наиболее распространенные угрозы информационной безопасности. Виды мер обеспечения информационной безопасности.

Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности

Обзор российского законодательства в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Морально-этические нормы поведения в цифровом мире. Организационно-правовые механизмы обеспечения информационной безопасности предприятия. Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5.12.2016 г. Закон 149-ФЗ «Об информации…». Закон 1-ФЗ «Об электронной цифровой подписи». Закон 63-ФЗ «Об электронной подписи». Обзор зарубежного законодательства в области информационной безопасности. Сетевые сервисы безопасности по уровням модели OSI. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки информационной безопасности ISO/IEC 15408. Российское и международное законодательство в области защиты прав на интеллектуальную собственность.

Тема 3. Административный и процедурный уровни обеспечения информационной безопасности

Анализ рисков информационной безопасности. Политика информационной безопасности. Программа работ в области обеспечения информационной безопасности. Основные классы мер процедурного уровня: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Тема 4. Программно-технические меры обеспечения информационной безопасности

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Технологии защиты данных. Идентификация и аутентификация, управление доступом. Шифрование, контроль целостности. Криптографические алгоритмы. Анализ защищенности. Обеспечение высокой доступности. Сервисы безопасности. Классификация сервисов безопасности с точки зрения места в общей архитектуре мер безопасности. Технологии защиты межсетевого обмена данными. Методы управления средствами сетевой безопасности.

Тема 5. Информационная безопасность в профессиональной деятельности

Организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия. Основные риски и угрозы информационной безопасности учреждений. Безопасное использование интернета в учреждении. Антивирусная защита информационных ресурсов учреждения. Контентная фильтрация. Защита персональных данных. Создание системы защиты информации в организации: этапы создания системы защиты информации, классификация организационно-технологических мероприятий по защите информации, общие требования к системе защиты информации. Защита экономических систем. Структура банковских информационных систем в области защиты информации.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/ практических занятий и контрольные мероприятия

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
1.	Тема 1. Основы информационной безопасности и защиты	Лекция № 1. Основы информационной безопасности и защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	-	2

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
	информации Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности Тема 3. Административный и процедурный уровни обеспечения информационной безопасности	Лекция № 2. Организационно-правовые механизмы обеспечения информационной безопасности предприятия	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	-	2
		Лекция № 3. Стандарты и спецификации в области информационной безопасности	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	-	4
		Практическое занятие № 1. Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	защита практической работы № 1, устный опрос № 1	10
2.	Тема 4. Программно-технические меры обеспечения информационной безопасности	Лекция № 5. Технологии защиты информации. Криптография. Электронная цифровая подпись	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	-	4
		Практическое занятие № 2. Шифрование. Идентификация и аутентификация. Сетевые сервисы Web 2.0: создание ментальных карт и др.	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	защита практической работы № 2, устный опрос № 2	12
3.	Тема 5. Информационная безопасность в профессиональной деятельности	Лекция № 6. ИБ инфраструктуры предприятия	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	-	2
		Лекция № 7. Основные риски и угрозы информационной безопасности учреждений	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	-	2
		Практическое занятие № 3. Защита информационных систем	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3	защита практической работы № 3, устный опрос № 3	12

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1.	Тема 1, 2, 3. Основы информационной безопасности и защиты информации.	1. Актуальность проблемы обеспечения безопасности в цифровом обществе, в условиях цифровой экономики и цифровизации сельского хо-

№ п/п	№ темы	Перечень рассматриваемых вопросов для самостоятельного изучения
	Законодательный и нормативно-правовой уровни обеспечения информационной безопасности. Административный и процедурный уровни обеспечения информационной безопасности	зяйства. 2. Законодательные акты РФ, регулирующие правовые отношения в сфере информационной безопасности и защиты государственной тайны. 3. Морально-этические нормы поведения в цифровом мире. 4. Политика информационной безопасности. Программа работ в области обеспечения информационной безопасности. ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3
2.	Тема 4. Программно-технические меры обеспечения информационной безопасности	1. Методы управления средствами сетевой безопасности. 2. Технологии обнаружения вторжений. 3. Инфраструктура защиты на прикладном уровне. 4. Технологии межсетевых экранов. 5. Обеспечение безопасности операционных систем. 6. Технологии аутентификации ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3
3.	Тема 5. Информационная безопасность в профессиональной деятельности	1. Основные риски и угрозы информационной безопасности учреждений. 2. Создание системы защиты информации в организации: этапы создания системы защиты информации, классификация организационно-технологических мероприятий по защите информации, общие требования к системе защиты информации. 3. Защита экономических систем. ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.3

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1.	Организационно-правовые механизмы обеспечения информационной безопасности предприятия.	Л	Интерактивная лекция
2.	Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.	ПЗ	Групповое обсуждение
3.	Защита информационных систем	ПЗ	Групповое обсуждение

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
4	Основные риски и угрозы информационной безопасности учреждений.	Л	Интерактивная лекция

6. Текущий контроль успеваемости и промежуточная аттестация по итогам освоения дисциплины

6.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

1) Примеры заданий практических работ

Пример задания по теме 2,3 : «Законодательный и нормативно-правовой уровни обеспечения информационной безопасности». «Административный и процедурный уровни обеспечения информационной безопасности»

Используя информационную систему Консультант Плюс, найти и отобразить с добавлением в раздел «Избранное» и экспортом в Microsoft Word:

1) основные нормативно-правовые акты, регулирующие деятельность в информационной сфере.

2) определения основных категорий информационной безопасности.

3) подборку статей по защите информации.

Примеры заданий по теме 4. «Программно-технические меры обеспечения информационной безопасности»

Пример 1. Используя справочные средства операционной системы Windows найти и отобразить с экспортом в Microsoft Word:

1) понятия учетной записи и домена и типов доступа к операционной системе: глобальные, локальные, ограниченные и административные.

2) описание порядка создания, изменения, активации и удаления учетных записей.

3) основные категории локальных пользователей (пользователи и группы) и конкретных прав каждого вида учетных записей, включая администраторов, пользователей, опытных пользователей, операторов архива, репликаторов и гостей.

Пример 2. Используя средства Internet (kaspersky.ru и т.п.), справочные средства и антивирусное программное обеспечение:

1) найти и отобразить с экспортом в Microsoft Word понятия мошеннического программного обеспечения, хакерских атак, фишинга и спама.

2) найти и отобразить с экспортом в Microsoft Word описание порядка использования и ключевых функций Kaspersky Unlocker и Kaspersky Internet Security, дать сравнительную характеристику ключевых функций Kaspersky

Rescue Disk и Kaspersky Antivirus (Kaspersky Virusscanner, Kaspersky Virus Removal Tool и т.д.).

3) открыть антивирусную программу, произвести настройку параметров ее работы, запустить проверку и сформировать отчет о результатах работы.

Пример 3.

1. Зашифровать следующие сообщения методом перестановки:
   ИНФОРМАЦИОННЫЕ СИСТЕМЫ
   ТЕЛЕКОММУНИКАЦИИ.
2. Зашифровать следующие сообщения методом подстановки:
   КОНФИДЕНЦИАЛЬНОСТЬ
   ШИФРОВАНИЕ
   КРИПТОГРАФИЯ
3. Расшифровать следующее сообщение методом перестановки без ключа:
   ЕЫНЬЛАНОСРЕП НАДЕЫН

Пример 4. Используя средства Internet и справочные средства программ резервного копирования найти и отобразить с экспортом в Microsoft Word:

1) понятия полного, дифференциального и инкрементного резервного копирования.

2) описание порядка создания образа и восстановления из него.

3) дать сравнительную характеристику основных функций трех программ резервного копирования по следующим критериям: условия распространения, планирование (работа по расписанию), возможности работы с разделами диска, создания загрузочного диска, шифрования, сжатия, настройки фильтров, онлайн резервного копирования.

Пример 5. Использование сетевых сервисов Веб 2.0.

1. Создание ментальной карты (https:// www.mindmup.com) на тему: «Виды вредоносных программ и методы защиты от них».
2. Создание вебмикса (https:// www.symbaloo.com) для реализации проекта «Интернет: проблемы защиты интеллектуальной собственности».
3. Использование сервиса ленты времени (https:// www.sutori.com) по истории развития компьютерных вирусов.

Примеры заданий по теме 5. «Информационная безопасность в профессиональной деятельности»

1. Запустить программу «1С: Предприятие» и продемонстрировать возможности решения вопросов информационной безопасности на уровне пользовательского интерфейса и в режиме «Конфигуратор».

2. Выполнить анализ и подготовить рекомендации по построению системы защиты АИС для заданной предметной области. Результатом выполнения теоретического задания должен быть перечень рекомендаций для обеспечения комплексной безопасности заданной предметной области. Практическое задание состоит в программной реализации криптографического метода (ассиметричный алгоритм RSA) защиты.

Примерная тематика заданий:

1. Система информационной безопасности для ИС для учета движения товаров на складе мелкооптовой торговли.
2. Система информационной безопасности для ИС для автоматизации обработки платёжных поручений.
3. Система информационной безопасности для ИС для учета расчетов по кредитам физических лиц коммерческого банка.
4. Система информационной безопасности для ИС составления сметы на ремонтно-строительные работы.
5. Система информационной безопасности для ИС агентства трудоустройства.

Темы проектов, реализуемых в рамках изучения дисциплины «Информационная безопасность»:

1. Исследовательские проекты: «Будущее цифровых денег. Информационная безопасность блокчейн»; «Здоровье интернета»; «Последствия DDOS-атак»; «Меры предупреждения угроз в сфере информационной безопасности».
2. Образовательные проекты: мастер-класс «Защита мобильного устройства», круглый стол «Современные уязвимости в сфере информационной безопасности», кейс реальной ситуации, которая могла произойти в сфере информационной безопасности».
3. Технологические проекты: «разработка инфраструктуры информационной безопасности предприятия», разработка политики и программы информационной безопасности «Цифровое и безопасное предприятие».
4. Программные проекты: «разработка (проектирование) обучающей программы по информационной безопасности», разработка мобильного приложения для обеспечения информационной безопасности в беспроводных локальных сетях.

2) Вопросы для устного опроса

Устный опрос № 1.

Тема 1. Основы информационной безопасности и защиты информации

Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности

Тема 3. Административный и процедурный уровни обеспечения информационной безопасности

1. Понятие информационной безопасности
2. Субъекты и объекты информационной безопасности
3. Понятие и функции системы защиты информации
4. Общие принципы обеспечения информационной безопасности
5. Специальные принципы обеспечения информационной безопасности
6. Обеспечивающие подсистемы защиты информации
7. Нормативно-правовые основы информационной безопасности

1. Понятие информационной угрозы
2. Причины реализации информационных угроз
3. Виды реализации угроз информационной безопасности
4. Классификация информационных угроз

5. Способы воздействия информационных угроз
8. Прогресс информационных технологий и необходимость обеспечения
9. безопасности
10. Основные понятия информатизации общества и информационной безопасности
11. Структура понятия «Информационная безопасность»
12. Субъекты и объекты информационной безопасности
13. Нормативно-правовое регулирование информационной безопасности
14. Стандарты и спецификации в области информационной безопасности.
15. Типы международных организаций в сфере информационной безопасности
16. Направления работы крупных альянсов в сфере информационной безопасности
17. Понятие и особенности экономической информации как объекта безопасности
18. Перечень сведений, относящихся к коммерческой тайне
19. Перечень сведений, которые не могут составлять коммерческую тайну
20. Объекты банковской тайны
21. Статьи Уголовного кодекса о компьютерных преступлениях
22. Доктрина информационной безопасности РФ
23. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации»
24. Федеральный закон от №63-ФЗ «Об электронной подписи»
25. 16. Принципиальные подходы к обеспечению информационной безопасности
26. Сравнительная характеристика фрагментного и комплексного подхода к защите
27. информации
28. Общие принципы обеспечения информационной безопасности
29. Специфические методы обеспечения информационной безопасности
30. Принципы построения системы информационной безопасности
31. Системный подход к защите информации
32. Требования к системе мер защиты информации
33. Принципы построения и особенности практической реализации системы защиты информации экономического субъекта
34. Механизм обеспечения информационной безопасности РФ в сфере экономики
35. Цели, задачи и функции системы защиты информации
36. Обеспечивающие компоненты системы защиты информации
37. Методы и средства обеспечения информационной безопасности
38. Российское и международное законодательство в области защиты прав на интеллектуальную собственность.
39. Анализ рисков информационной безопасности.

Устный опрос № 2.

Тема 4. Программно-технические меры обеспечения информационной безопасности

1. Классификация вредоносного программного обеспечения
2. Классификация компьютерных преступлений
3. Методы обеспечения информационной безопасности
4. Средства обеспечения информационной безопасности
5. Криптографическое обеспечение информационной безопасности
6. Организационное обеспечение информационной безопасности
7. Особенности и этапы построения системы защиты информации
8. Методы реализации механизмов защиты информации
9. План построения системы защиты информации
10. Функции службы информационной безопасности
11. Симметричные криптосистемы. AES. ГОСТ.
12. Ассиметричные криптосистемы. RSA. El Gamal.
13. Криптографические протоколы. Общие понятия, типы криптопротоколов.
14. Протоколы аутентификации. Слабости парольных протоколов аутентификации. Виды атак и угроз для протоколов аутентификации. Полнота, корректность. Стойкость протокола.
15. Протокол аутентификации Фейге – Фиата - Шамира. Анализ протокола.
16. Протокол аутентификации Шнорра. Анализ протокола. Рекомендации по использованию. Сфера применения протокола.
17. Протоколы электронной подписи. Общие понятия и определения. Виды атак и угроз для протоколов электронной подписи. Стойкость протокола.
18. Криптографические хэш-функции. Определение и требования к ним. Задача вычисления коллизий хэш-функций. Атаки и угрозы для хэш-функций, стойкость хэш-функции. Области применения хэш-функций.
19. Хэш-функция SHA. Построение хэш-функций на основе стойких криптосистем.
20. Использование хэш-функций в протоколах электронной подписи. Протокол электронной подписи DSS.
21. Электронная подпись в системе RSA.
22. Архитектура системы безопасности ОС Windows.
23. Архитектура системы безопасности ОС Windows
24. Субъект доступа.
25. Объект доступа.
26. Механизм контроля доступа.
27. Диспетчер учётных записей SAM. Пароли и ключи пользователей.
28. База учётных записей SAM: типичные атаки и методы её защиты.
29. Введение в файловую систему NTFS. Права доступа стандартные, специфичные и родовые.
30. Разрешения NTFS индивидуальные, стандартные и специальные.
31. Механизм наследования разрешений. Средства редактирования разрешения NTFS.
32. Шифрование данных в NTFS. Рекомендации по защите средствами NTFS.
33. Безопасность сервера SMB. Введение в протокол SMB

34. Типичные атаки на протокол и методы защиты. Аудит сервера SMB.
35. Проверка подлинности при входе в домен Windows.
36. Защита реестра Windows.
37. Безопасность серверов RAS и IIS.
38. Инфраструктура открытых ключей PKI
39. Протокол KERBEROS
40. Криптоинтерфейс, криптопровайдеры
41. Защищенные протоколы и защищенные компьютерные системы
42. Удаленные атаки на защищенные компьютерные системы и методы защиты от них.

Устный опрос № 3.

Тема 5. Информационная безопасность в профессиональной деятельности

1. Обеспечение информационной безопасности информационных систем банков
2. Обеспечение информационной безопасности электронной коммерции
3. Обеспечение информационной безопасности учетной деятельности

3) Перечень вопросов, выносимых на экзамен

1. Прогресс информационных технологий и необходимость обеспечения безопасности
2. Основные понятия информатизации общества и информационной безопасности
3. Структура понятия «Информационная безопасность»
4. Субъекты и объекты информационной безопасности
5. Типы международных организаций в сфере информационной безопасности
6. Направления работы крупных альянсов в сфере информационной безопасности
7. Понятие и особенности экономической информации как объекта безопасности
8. Перечень сведений, относящихся к коммерческой тайне
9. Перечень сведений, которые не могут составлять коммерческую тайну
10. Объекты банковской тайны
11. Статьи Уголовного кодекса о компьютерных преступлениях
12. Доктрина информационной безопасности РФ
13. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации»
14. Федеральный закон от №63-ФЗ «Об электронной подписи»
15. Принципиальные подходы к обеспечению информационной безопасности
16. Сравнительная характеристика фрагментного и комплексного подхода к защите информации
17. Общие принципы обеспечения информационной безопасности
18. Специфические методы обеспечения информационной безопасности
19. Принципы построения системы информационной безопасности

20. Системный подход к защите информации
21. Требования к системе мер защиты информации
22. Принципы построения и особенности практической реализации системы защиты информации экономического субъекта
23. Механизм обеспечения информационной безопасности РФ в сфере экономики
24. Цели, задачи и функции системы защиты информации
25. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
26. Защита интеллектуальной собственности средствами патентного и авторского права.
27. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
28. Симметричные шифры.
29. Ассиметричные шифры.
30. Криптографические протоколы.
31. Криптографические хеш-функции.
32. Электронная подпись.
33. Организационное обеспечение информационной безопасности.
34. Служба безопасности организации.
35. Обеспечивающие компоненты системы защиты информации
36. Методы и средства обеспечения информационной безопасности
37. Сущность криптографических методов
38. Организационно-административные мероприятия обеспечения компьютерной безопасности
39. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения
40. Меры предупреждения и защиты от компьютерных преступлений
41. Информационные угрозы и их классификация
42. Действия и события, нарушающие информационную безопасность
43. Основные виды каналов утечки информации
44. Пути несанкционированного доступа к информации
45. Стратегия и тактика злоумышленника при несанкционированном доступе
46. Личностно - профессиональные характеристики сотрудников, способствующие реализации информационных угроз
47. Способы воздействия угроз на информационные объекты
48. Вредоносные программы, их виды
49. Признаки воздействия вирусов на компьютерную систему
50. Исторические аспекты компьютерных преступлений
51. Уголовно-правовая характеристика компьютерных преступлений,
52. Компьютерные преступления и их классификация
53. Субъекты компьютерных преступлений
54. Объективная сторона компьютерных преступлений
55. Уголовно-правовой контроль над компьютерной преступностью в РФ
56. Организация системы защиты информации экономических систем
57. Этапы построения системы защиты информации

58. Политика информационной безопасности
59. Способы практической реализации механизмов защиты информации
60. План построения системы защиты информации
61. Организация конфиденциального делопроизводства
62. Структура и функции службы информационной безопасности компании
63. Типы политики информационной безопасности
64. Оценка эффективности инвестиций в информационную безопасность
65. Обеспечение информационной безопасности автоматизированных банковских систем
66. Информационная безопасность электронной коммерции
67. Обеспечение компьютерной безопасности учетной информации
68. Информационная безопасность предпринимательской деятельности
69. Методика защиты электронной почты
70. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов
71. Электронная цифровая подпись и особенности ее применения
72. Защита информации в Интернете
73. Информационная безопасность пользователей мобильных устройств

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенций по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При использовании традиционной системы контроля и оценки успеваемости студентов представлены критерии выставления оценок по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Промежуточный контроль знаний проводится в форме экзамена.

Критерии оценки экзамена представлены в таблицах 7, 8.

Таблица 7

Промежуточный контроль знаний обучающихся

Шкала оценивания	Экзамен
5	Отлично
4	Хорошо
3	Удовлетворительно
2	Неудовлетворительно

Таблица 8

Критерии оценки экзамена

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	Оценку «**отлично**» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов, на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.

Оценка	Критерии оценивания
	Студент самостоятельно и полностью раскрывает сущность теоретических вопросов, самостоятельно использует возможности программных средств для решения прикладных задач; самостоятельно подтверждает ответ конкретными примерами и заданиями; правильно и обстоятельно отвечает на дополнительные вопросы преподавателя.
Средний уровень «4» (хорошо)	Оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, в основном сформировал практические навыки. Студент допускает незначительные ошибки в заданиях и ответах; самостоятельно использует основные функции программных средств; самостоятельно подтверждает ответ конкретными примерами и заданиями.
Пороговый уровень «3» (удовлетворительно)	Оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, некоторые практические навыки не сформированы. Студент не может самостоятельно использовать значительную часть функций программных средств, затрудняется подтвердить ответ конкретными примерами и заданиями; слабо отвечает на дополнительные вопросы.
Минимальный уровень «2» (неудовлетворительно)	Оценку **«неудовлетворительно»** заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, практические навыки не сформированы. Студент не может использовать программные средства при решении различных задач; не может подтвердить ответ конкретными примерами и заданиями; не отвечает на дополнительные вопросы преподавателя.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. – 5-е изд., стер. – Санкт-Петербург: Лань, 2019. – 324 с. – ISBN 978-5-8114-4067-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/114688 (открытый доступ).

2. Информационная безопасность: учебное пособие / составители Е. Р. Кирколуп [и др.]. – Барнаул: АлтГПУ, 2017. – 316 с. – ISBN 978-5-88210-898-3. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/112164 (открытый доступ).

3. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. – 2-е изд. – Москва: ИНТУИТ, 2016. – 266 с. – ISBN 978-5-94774-821-5. – Текст: электронный //Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/100295 (открытый доступ).

7.2 Дополнительная литература

1. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум: учебное пособие / Р. Н. Гилязова. – Санкт-Петербург: Лань, 2020. – 44 с. – ISBN 978-5-8114-4294-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/130179 (открытый доступ).

2. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург: Лань, 2020. – 124 с. – ISBN 978-5-8114-4404-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/133924 (открытый доступ).

3. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие / С. Н. Никифоров. – 2-е изд., стер. – Санкт-Петербург: Лань, 2019. – 96 с. – ISBN 978-5-8114-4040-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/114697 (открытый доступ).

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Бесплатное дистанционное обучение в Национальном Открытом Университете «ИНТУИТ» [Электронный ресурс]. – Режим доступа: http://www.intuit.ru (открытый доступ).

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф. – Электрон. Текстовые данные. – Саратов: Профобразование, 2017. – 544 с. – Режим доступа: http://www.iprbookshop.ru/63592.html (открытый доступ).

9. Перечень программного обеспечения и информационных справочных систем

1. 1 Справочная правовая система «КонсультантПлюс» (открытый доступ): [Электронный ресурс]. – Режим доступа: www.consultant.ru. – Загл. с экрана.

Таблица 9

Перечень программного обеспечения

Наименование темы учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
По всем темам дисциплины	Microsoft Windows 7 и выше	Операционная система	Microsoft	2009
	Microsoft Office 2010 и выше	Пакет офисных программ		2010
	Google Chrome	Браузер		2012

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения лекционных и практических занятий по дисциплине «Информационная безопасность» необходимы аудитория и компьютерный класс, подключенные к сети Интернет, оснащенные средствами мультимедиа и программными средствами: MS Windows 7/8/10; MS Office 2007/2010/2013/365 (Office Online), системой КонсультантПлюс, программой демонстрации NetOp School, браузером Google Chrome.

Лекции проводятся в специализированной аудитории, оборудованной мультимедийным проектором для демонстрации компьютерных презентаций.

Для проведения практических занятий по дисциплине «Информационная безопасность» необходим компьютерный класс с установленными на ПК программным обеспечением, указанным в п. 9.

Таблица 10

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
1	2
Аудитория для проведения занятий лекционного типа № 118 - уч. корпус № 15	Видеопроектор 3500 Лм
Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №УИТ-113, уч. корпус №15	Персональные компьютеры в количестве 20 штук
Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №УИТ-110, уч. корпус №15	Персональные компьютеры в количестве 20 штук
Аудитория для проведения практических	Персональные компьютеры (терминалы) в

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
1	2
занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №УИТ-114, уч. корпус №15	количестве 20 штук
Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №УИТ-102, уч. корпус №15	Персональные компьютеры (терминалы) в количестве 20 штук
Центральная научная библиотека имени Н.И. Железнова	Читальные залы библиотеки
Общежитие	Комната для самоподготовки

11. Методические рекомендации студентам по освоению дисциплины

Изучение учебной дисциплины «Информационная безопасность» включает освоение материалов лекций, приобретение практических навыков работы с программными средствами.

На лекциях при помощи мультимедиа проектора и презентаций раскрываются основные теоретические вопросы дисциплины, делаются акценты на наиболее сложные положения изучаемого материала.

Лекционный материал следует просматривать и изучать по конспекту/электронной презентации самостоятельно после аудиторных занятий. Для более углубленного изучения материала необходимо использовать рекомендованную литературу и Интернет-ресурсы.

Практические занятия проводятся в компьютерных классах с применением методических материалов. На занятиях необходимо иметь электронный носитель информации – флэш-карту для сохранения результатов своей работы. Учебные материалы можно сохранять в облачных сервисах: Google Диск, Яндекс.Диск, Облако Mail.Ru, Dropbox.

Посещение лекций и практических занятий – обязательно.

Консультирование по выполнению заданий практических работ проводится в компьютерных классах во время консультаций по графику (см. на стендах кафедры), а также через электронный обмен сообщениями с преподавателями, посредством Интернет и электронной информационно-образовательной среды Университета через личный кабинет.

Необходимо соблюдать сроки выполнения всех заданий.

Полученные оценки за выполненные задания являются основой для промежуточной аттестации.

Виды и формы отработки пропущенных занятий

Студент, обязан отработать:

– пропущенные лекции – представив преподавателю конспект лекции, ответив на вопросы устно, пройдя собеседование по пропущенной теме;

– пропущенные практические занятия – в форме выполнения заданий, устного опроса, посещения дополнительных занятий.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Учебный процесс по курсу «Информационная безопасность» включает следующие организационные формы: лекции, практические занятия и консультации, а также систему контроля знаний, самостоятельную работу студентов.

Методика чтения лекций зависит от цели и задач изучения предмета/раздела, а также уровня общей подготовки обучающихся, форма ее проведения – от характера темы и содержания материала. Высокая эффективность деятельности преподавателя во время чтения лекции достигается за счет глубокого освоения предметной области, педагогического мастерства, высокой речевой культуры и ораторского искусства, когда учитывается психология аудитории, закономерности восприятия, внимания, мышления, эмоциональные процессы учащихся, обратная связь и принципы дидактики.

При подготовке материала лекции преподавателю необходимо:

– учитывать требования государственного образовательного стандарта, учебного плана и рабочей программы;

– применять принципы дидактики (наглядность, от теории к практике, доступность, структуризация и систематизация и т.д.);

– уметь создавать интерактивные презентации;

– уметь использовать технические (проектор) и программные средства (например, программу подготовки презентаций MS PowerPoint, программу управления компьютерным классом NetOp School) и др.

Для проведения практических занятий преподавателю следует разрабатывать задания различной степени сложности, инструкции (методические указания) по выполнению каждого задания, раздаточный материал в печатном и электронном виде.

По курсу «Информационная безопасность» должны быть организованы:

– «очные» консультации в компьютерном классе, проводимые преподавателем согласно графику (размещается на стендах кафедры);

– off-line консультации, проводимые преподавателем с помощью электронной почты;

– взаимодействия в электронной информационно-образовательной среде Университета через личный кабинет.

Для организации контрольных мероприятий преподавателю следует подготовить вопросы для устного опроса и практические задания. Преподаватель должен использовать различные методы обучения:

– объяснительно-иллюстративный (лекция, объяснение, работа с учебником, демонстрация презентаций);

– репродуктивный (воспроизведение действий по применению знаний на практике, деятельность по алгоритму, программирование);

– частично-поисковый (поиск решения познавательных задач под руководством преподавателя);

– исследовательский метод, в котором после анализа материала, постановки проблем и задач и краткого устного или письменного инструктажа обучаемые самостоятельно изучают литературу, источники, ведут наблюдения и измерения и выполняют другие действия поискового характера.

– активные методы: групповое обсуждение, интерактивная лекция и др.