МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ
Декан, председатель совета факультета ИЭФ

_____ **Э.Б. Атуева**
подпись Ф.И.О
20.09 **2018г.**

УТВЕРЖДАЮ
Проректор по учебной работе, председатель методического совета ДГТУ

_____ **Н.С.Суракатов**
подпись Ф.И.О
24.09 **2018г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.В. ДВ3. Защита информации

для направления 38.03.01 Экономика

по профилю Экономика предприятий и организаций

факультет инженерно-экономический
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) бакалавр

Форма обучения очная ; курс 1 ; семестр(ы) 2 ;

Всего трудоемкость в зачетных единицах (часах) 2 ЗЕТ (72);

Лекции 17 (час); Экзамен - (-);

Практические (семинарские) занятия нет; Зачет 2 (семестр);

Лабораторные занятия 17 (час); Курсовая работа нет (семестр);

Самостоятельная работа 38 (час).

Зав. кафедрой ИБ _____ **Г.И. Качаева**

Начальник УО _____ **Э.В. Магомаева**

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению подготовки бакалавров 38.03.01 – «Экономика», профиля подготовки «Экономика предприятий и организаций».

Программа одобрена на заседании выпускающей кафедры экономики и управления на предприятии (ЭиУна П), протокол №2 от 19.09.2018г.

от 12.09.18 г., протокол № 1

Зав. выпускающей кафедрой по направлению подготовки бакалавров 38.03.01 – «Экономика»

_____ **Ж.Н.Казиева**

ОДОБРЕНО:

Методической комиссией по укрупненным группам специальностей и направлению подготовки

38.03.01 – Экономика и управление

АВТОР ПРОГРАММЫ

Качаева Г.И., ст.преп.

И.О.Ф., уч. степень, ученое звание

Председатель МК

Эсетова А.М. _____

подпись, И.О.Ф. подпись

12 09 2018г.

2. Цель освоения дисциплины

Цель дисциплины изучение методов и средств защиты информации, исключающих несанкционированный доступ к информации, хранящейся и обрабатываемой в ЭВМ, обеспечение информационной безопасности организации, обеспечение комплексной защиты объектов информации от различных угроз.

Задачами дисциплины являются: освоение методов и средств защиты компьютерной информации, изучение методов защиты программ от несанкционированного доступа, построение комплексных систем защиты.

В результате изучения дисциплины обучающийся должен:

Знать: основные понятия и определения в области защиты информации; концепции и методы защиты информации; источники, риски и формы атак на информацию; стратегии аутентификации и авторизации; концепции сетевого аудита; технологии обнаружения вторжения; стратегии политик безопасности; принципы сетевой обороны.

Уметь: анализировать угрозы и факторы, влияющие на безопасность информации в компьютере, компьютерной системе и сети; создавать план защиты информационных объектов и их информационного взаимодействия; выбирать и применять обоснованное средство защиты; обновлять систему безопасности с использованием служб обновления, планировать политику безопасности объекта информатизации.

Владеть:

конфигурированием параметров безопасности подсоединения системы к Интернет; использованием средств защиты файлов шифрованием; конфигурированием параметров аутентификации и авторизации; администрированием средств защиты информации; планированием защиты по периметру компьютерной сети.

2.Место дисциплины в структуре ООП бакалавриата

Дисциплина «Защита информации» относится к вариативной части учебного плана ФГОС ВО (дисциплина по выбору студента) . Изучение данной дисциплины базируется на следующих дисциплинах: "Информатика" и “Математика”. Студент должен знать характеристики компьютеров, математические основы изучаемых разделов.

Для освоения дисциплины «Защита информации» обучающимся необходимо:

Знать:

- системы счисления, особенности работы операционной системы и прикладных программ, компьютерные системы и сети;

Уметь:

- применять вычислительную технику для решения практических задач;
- понимать задачу, уметь использовать алгоритм ее решения;

- работать с современными компьютерными системам;

Владеть:

- навыками работы с программным обеспечением предназначенным для защиты информации.

3.Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

В результате освоения дисциплины «Защита информации» студент должен обладать следующими компетенциями

общекультурными:

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

профессиональными:

способностью на основе типовых методик и действующей нормативно-правовой базы рассчитывать экономические и социально-экономические показатели, характеризующие деятельность хозяйствующих субъектов (ПК-2);

способностью выполнять необходимые для составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми в организации стандартами (ПК-3);

способностью анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в отчетности предприятий различных форм собственности, организаций, ведомств и т.д., и использовать полученные сведения для принятия управленческих решений (ПК-5);

В результате изучения курса студент должен иметь представление: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности; о методологии создания систем защиты информации, о перспективных направлениях развития средств и методов защиты информации.

4. Структура и содержание дисциплины (модуля) «Защита информации»

Общая трудоемкость дисциплины составляет 2 зачетные единицы – 72 часа, в том числе: лекционных -17 часов, лабораторных - 17 часов, СРС -38 часов, форма отчетности зачет во 2 семестре.

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля (по срокам текущей аттестации)
				ЛК	ПЗ	ЛР	СРС	
1	2	3	4	5	6	7	8	9
1.	**Лекция 1.** **Тема: Основные понятия информационной безопасности.** 1. Основные причины обострения проблемы обеспечения информационной безопасности. 2. Основные составляющие понятия информационной безопасности.	2	1,2	2			4	Вх.контр.
2.	**Лекция 2.** **Тема: Классификация угроз безопасности информации.** 1. Основные определения и критерии классификации угроз. 2. Преднамеренные и непреднамеренные (случайные) угрозы.		3,4	2		2	6	
3.	**Лекция 3.** **Тема: Подходы к формированию политики безопасности.** 1. Задачи политики безопасности 2. Фрагментарный подход к формированию политики безопасности 3. Комплексный подход. Используемые меры при формировании политики безопасности.		5,6	2		4	8	АКР№1
4.	**Лекция 4.** **Тема: Фундаментальные технологии защиты информации. Криптографическая защита данных** 1. Криптография. Классификация криптографических алгоритмов 2. Симметричные и ассиметричные криптографические алгоритмы 3. Блочные и потоковые алгоритмы.		7,8	2		2	4	

5.	**Лекция 5.** **Тема: Защита системы от вредоносных программ.** 1. Защита программ от разрушающих программных воздействий. Классификация компьютерных вирусов, червей, спама, резидентов. 2. Способы обнаружения и защиты. Защита программ от изменения и контроль целостности. 3. Обзор существующего программного обеспечения для защиты от вредоносных программ.	2	9,10	2		2	4	АКР№2
6.	**Лекция 6.** **Тема: Базовые технологии безопасности данных** 1. Методы аутентификации и идентификация. Сетевая аутентификация на основе одноразового и многоразового пароля. 2. Электронная цифровая подпись. Процедуры проверки цифровой подписи. **3.** Управление доступом. Протоколирование и аудит.		11,12	2		2	4	
7	**Лекция 7.** **Тема: Законодательный уровень информационной безопасности.** 1. Обзор российского законодательства в области информационной безопасности. **2.** Обзор зарубежного законодательства в области информационной безопасности.		13,14	3		2	4	
8	**Лекция 8.** **Тема: Административный уровень информационной безопасности.** 1. Политика безопасности 2. Программа безопасности **3.** Синхронизация программы безопасности с жизненным циклом систем.		15,16	2		2	2	АКР№3
9	**Лекция 9. Тема: Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.** 1. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись. 2. Стандарты цифровой подписи ГОСТ 3410 и DSS.		17	1		1	2	
Итого				**17**		**17**	**38**	

Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторной работы	№ литер. источника из списка литературы	Кол-во часов
1	1,2	Исследование возможностей системы безопасности Windows XP по разграничению полномочий пользователей и в офисных приложениях Microsoft Office.	№ 1-17	2
2	3	Исследование методов криптографической защиты информации.	№ 1-17	4
3	4	Исследование методов криптографической защиты информации.	№ 1-17	2
4	5	Исследование программы шифрования данных TrueCrypt. Создание и использование файлового контейнера TrueCrypt.	№ 1-17	2
5	6	Сравнительный анализ эффективности антивирусных программных комплексов.	№ 1-17	2
6	7	Законодательный уровень информационной безопасности	№ 1-17	2
7	8	Административный уровень информационной безопасности	№ 1-17	2
8	9	Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.		1
		Итого за семестр:		**17**

4.2. Тематика для самостоятельной работы студента

№ п/п	**Тематика лабораторного практикума**	**Кол-во часов из содержания дисциплины**	**Рекомендуемая литература и источники информации**	**Форма контроля СРС**
1	Основные понятия информационной безопасности.	4	№ 1-17	Рефераft, АКР, Зачет
2	Классификация угроз безопасности информации.	6	№ 1-17	Рефераft, АКР, Зачет
3	Подходы к формированию политики безопасности.	8	№ 1-17	Рефераft, АКР, Зачет
4	Фундаментальные технологии защиты информации. Криптографическая защита данных.	4	№ 1-17	Рефераft, АКР, Зачет
5	Защита системы от вредоносных программ.	4	№ 1-17	Рефераft, АКР, Зачет
6	Базовые технологии безопасности данных.	4	№ 1-17	Рефераft, АКР, Зачет
7	Законодательный уровень информационной безопасности.	4	№ 1-17	Рефераft, АКР, Зачет

8	Административный уровень информационной безопасности.	2	№ 1-17	Рефераft, АКР, Зачет
9	Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.	2	№ 1-17	Рефераft, АКР, Зачет
	Итого	**38**		

5.Образовательные технологии

В соответствии с требованиями ФГОС ВПО по направлению подготовки 38.03.01 Экономика (квалификация (степень) «бакалавр») удельный вес занятий, проводимых в интерактивных формах, составляет 10% аудиторных занятий, при этом занятия лекционного типа составляют 16% аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Вопросы входного контроля для проверки знаний студентов

1. Запишите в двоичной системе счисления заданное в десятичной системе число.
2. Что показывает кодовая таблица ЭВМ?
3. Что понимается под байтовым алфавитом?
4. В каком виде существует информация в ЭВМ?
5. По какому правилу текстовая информация превращается в цифровую для ввода в ЭВМ?

Контрольные вопросы для проверки текущих знаний студентов

Аттестационная контрольная работа № 1

1. Службы сертификации. Центры сертификации. Управление сертификатами.
2. Аутентификации, авторизация и администрирование (AAA) доступа к данным.
3. Методы аутентификации, использующие пароли и сертификаты.
4. Протоколы аутентификации на основе симметричного шифрования.
5. Строгая аутентификации, основанная на асимметричном шифровании.
6. Планирование и реализация стратегии аутентификации.
7. Управление доступом к данным.
8. Аудит безопасности. Шаблоны безопасности.
9. Методы защиты передачи данных.
10. Стратегии защиты удалённого доступа к ресурсам инфосистемы.
11. Анализ уязвимостей удаленного доступа.
12. Планирование и настройка требуемого уровня безопасности для информационных серверов.
13. Протоколы безопасности.
14. Структуры пакетов для транспортного и туннельного режимов.

Аттестационная контрольная работа №2

1. Защита программ от разрушающих программных воздействий.
2. Классификация компьютерных вирусов, червей, спама, резидентов.
3. Жизненный цикл. Виды антивирусных программ, критерии качества.
4. Способы обнаружения и защиты.
5. Защита программ от изменения и контроль целостности.
6. Атаки. Программные средства атак.
7. Обобщенная структура и компоненты системы обнаружения атак.
8. Симметричные и асимметричные криптосистемы шифрования.
9. Электронные цифровые подписи.
10. Функции хэширования.
11. Комбинированные криптосистемы.
12. Управление ключами.
13. Методы и средства хранения и распределения ключей.

Аттестационная контрольная работа №3

1. Основные принципы построения, характеристики и классификация программно-аппаратных средств защиты информации.
2. Анализ требований к защите информации.
3. Оценка потенциальных угроз и уязвимости информации на разных этапах ее обработки, хранения, передачи.
4. Анализ рисков.
5. Предварительный сбор данных и сканирование системы.
6. Политика сетевой безопасности.
7. Этапы создания политики безопасности.
8. Структуры систем защиты компьютера и сети

Перечень вопросов к зачету

1. Основные принципы построения, характеристики и классификация программно-аппаратных средств защиты информации.
2. Анализ требований к защите информации.
3. Оценка потенциальных угроз и уязвимости информации на разных этапах ее обработки, хранения, передачи.
4. Анализ рисков.
5. Предварительный сбор данных и сканирование системы.
6. Меры противодействия зондированию, методы защиты от атак.
7. Методы защиты программного обеспечения от изучения.
8. Способы анализа программ и методы противодействия изучению, способы встраивания средств защиты в программное обеспечение.
9. Политика сетевой безопасности.
10. Этапы создания политики безопасности.
11. Структуры систем защиты компьютера и сети.
12. Симметричные и асимметричные криптосистемы шифрования.
13. Электронные цифровые подписи.
14. Функции хэширования.
15. Комбинированные криптосистемы.
16. Управление ключами.
17. Методы и средства хранения и распределения ключей.
18. Типовые решения в организации ключевых систем.
19. Имитозащита информации.
20. Компоненты инфраструктуры открытых ключей.

21. Службы сертификации. Центры сертификации. Управление сертификатами.
22. Типы сертификатов. Запрос, импорт, экспорт сертификатов. Хранилище сертификатов.
23. Аутентификации, авторизация и администрирование (AAA) доступа к данным.
24. Управление доступом к данным.
25. Стандартные и специальные права доступа.
26. Наследование разрешений и запретов.
27. Базовая стратегия использования групп.
28. Аудит безопасности. Шаблоны безопасности.
29. Методы защиты передачи данных.
30. Стратегии защиты удалённого доступа к ресурсам инфосистемы.
31. Анализ уязвимостей удаленного доступа.
32. Политики удалённого доступа.
33. Централизованное управление удалённым доступом.
34. Протоколы туннелирования, инкапсуляции данных. Настройка политик на соединяющихся сторонах.
35. Защита программ от разрушающих программных воздействий.
36. Классификация компьютерных вирусов, червей, спама, резидентов.
37. Жизненный цикл. Виды антивирусных программ, критерии качества.
38. Способы обнаружения и защиты.
39. Защита программ от изменения и контроль целостности.
40. Примеры антивирусных программных комплексов. Методы защиты от спама.

Вопросы для проверки остаточных знаний

1. Понятие угрозы и атаки. Классификации угроз. Уязвимость информации на разных этапах ее обработки, хранения, передачи.
2. Политика безопасности. Подходы к формированию политики безопасности.
3. Протоколирование и аудит.
4. Электронные цифровые подписи.
5. Аутентификации и идентификация.
6. Аудит безопасности. Шаблоны безопасности.
7. Криптографическая защита информации.
8. Симметричные и асимметричные криптосистемы шифрования.
9. Вирусы и их классификация.
10. Примеры антивирусных программных комплексов. Методы защиты от спама.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Дагестанский Государственный Технический Университет»

Кафедра Информационная безопасность

ТЕСТ

_____ТА_____
(ТА – текущая аттестация, ПА – промежуточная аттестация, ИА – итоговая аттестация)

по дисциплине «Защита информации**»**

Перечень специальностей, для которых планируется использование педагогические тестовые материалы

38.03.01 - «Экономика»
Наименование направления

Составители: Качаева Г.И.
Ф.И.О. разработчика

Махачкала 2018

Содержание теста по дисциплине
«Защита информации»

1. Что такое информация?
   a) **сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах.Это информационная система, обеспечивающая сбор, отображение пространственных данных**
   b) Быстро развивающиеся компьютерные информационные технологии
   c) сведения, передаваемые между людьми, человеком и автоматом, автоматом и автоматом
   d) признаки, передаваемые от клетки к клетке, от организма к организму.

2. Под термином **информационная безопасность** понимается:
   a) Сбор, хранение, обработку, анализ и отображение временных данных на носителях
   b) **состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений**
   c) обеспечение конфиденциальности, целостности и достоверности обрабатываемых данных
   d) свойство информации, гарантирующее, что лица имеющие доступ к информации в нужный момент смогут получить доступ

3. Определение конфиденциальной информацией:
   a) **документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации**
   b) такая документированная информация, доступ к которой не ограничивается в соответствии с законодательством Российской Федерации
   c) сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах
   d) информация, доступ к которой имеют только определенные лица.

4. Что такое **Конфиденциальность**?
   a) свойство информации, гарантирующее, что лица имеющие доступ к информации в нужный момент смогут получить доступ
   b) свойство это свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения в неискаженном виде по отношению к некоторому фиксированному состоянию .
   c) комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности
   d) **свойство информации, гарантирующее, что доступ к информации имеет доступ только определенные лица.**

5. Что такое Целостность?
    a) свойство информации, гарантирующее, что лица имеющие доступ к информации в нужный момент смогут получить доступ
    b) свойство это свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения в неискаженном виде по отношению к некоторому фиксированному состоянию .
    c) комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности
    d) свойство информации, гарантирующее, что доступ к информации имеет доступ только определенные лица.

6. Что такое Доступность?
    a) свойство информации, гарантирующее, что лица имеющие доступ к информации в нужный момент смогут получить доступ
    b) свойство это свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения в неискаженном виде по отношению к некоторому фиксированному состоянию .
    c) комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности
    d) свойство информации, гарантирующее, что доступ к информации имеет доступ только определенные лица.

7. Что такое Защита информации ?
    a) Совокупность сведений, определяющих меру наших знаний об объекте
    b) Совокупность фактов, известных об объектах, либо результаты измерения этих объектов.
    c) комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.
    d) Разграничение доступа к информации

8. Понятие Угрозы информационной безопасности.
    a) Преднамеренная реализация угрозы
    b) потенциальная возможность нарушения режима информационной безопасности
    c) следствием наличия уязвимых мест в защите информационных систем
    d) Сведения, определяющих меру наших знаний об объекте

9. Что называется атакой на информационную систему:
    a) Преднамеренная реализация угрозы
    b) потенциальная возможность нарушения режима информационной безопасности
    c) следствием наличия уязвимых мест в защите информационных систем
    d) Сведения, определяющих меру наших знаний об объекте

10. Угрозы информационной безопасности классифицируются по следующим признакам:

a) по составляющим ИБ, по характеру воздействия, по расположению источника угроз;
b) по составляющим ИБ, по компонентам ИС, по характеру воздействия, по расположению источника угроз;
c) по составляющим ИС, по характеру воздействия, по расположению источника угроз;
d) по составляющим ИБ, по компонентам ИС, по характеру воздействия;

11. **Угрозы по характеру воздействия могут быть**:

a) ошибочными
b) случайными
c) преднамеренными
d) аварийными

12. По расположению источника угрозы бывают:

a) внутренние
b) внешние
c) случайные
d) преднамеренные

13. Каналы НСД не относящиеся к компонентам АИС:

a) программные
b) аппаратные
c) физического воздействия
d) случайные

14. Подходы к проблеме обеспечения безопасности АСОИ:

a) Фрагментарый и комплексный.
b) противодействие четко определенным угрозам в заданных условиях .
c) Природопользовательские, региональные
d) Различные виды пространственного воздействия

15. Фрагментарный" подход направлен на:

a) на создание защищенной среды обработки информации в АСОИ
b) противодействие четко определенным угрозам в заданных условиях.
c) Анализ пространственных данных или пространственный анализ
d) основан на разработанной для конкретной АСОИ политики безопасности.

16. Фрагментарные меры защиты информации обеспечивают:

a) защиту конкретных объектов АСОИ только от конкретной угрозы.
b) основан на разработанной для конкретной АСОИ политики безопасности.
c) ограничения на свободу действий пользователей АСОИ.
d) большая чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Комплексный подход ориентирован на:

a) защиту конкретных объектов АСОИ
b) высокуюизбирательность к конкретной угрозе
c) четко определенные угрозы в заданных условиях
d) создание защищенной среды обработки информации в АСОИ.

17. Политика информационной безопасности представляет:

a) все аспекты информационных технологий
b) набор норм, правил и практических рекомендаций, на которых строится управление информации
c) набор норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в АСОИ
d) совокупность массивов информации, систем кодирования и классификациюинформации.

18. Виды политики безопасности

a) Избирательная и полномочная.
b) рабочая
c) пользовательская
d) внешняя

19. Методы защиты информации:

a) государственные, административные, физические, программно-технические методы
b) Внешние, внутренние.
c) Правовые, морально-этические, административные, физические, программно-технические;
d) Физические, технические, политические. Экологические. экономические

20. К правовым мерам защиты информации относятся:

a) меры организационного характера
b) действующие законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и мер ответственности за их нарушения .
c) всевозможные нормы поведения, которые традиционно сложились в обществе
d) разного рода механические, электрические и электронно-механические устройства

21. К административным мерам защиты информации относятся:

a) действующие законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и мер ответственности за их нарушения **.**
b) меры организационного характера
c) всевозможные нормы поведения, которые традиционно сложились в обществе
d) разного рода механические, электрические и электронно-механические устройства

22. К морально-этическим мерам защиты информации относятся:

a) действующие законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и мер ответственности за их нарушения
b) меры организационного характера
c) разного рода механические, электрические и электронно-механические устройства
d) всевозможные нормы поведения, которые традиционно сложились в обществе

23. К физическим мерам защиты информации относятся:
a) действующие законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и мер ответственности за их нарушения **.**
b) меры организационного характера
c) всевозможные нормы поведения, которые традиционно сложились в обществе
d) разного рода механические, электрические и электронно-механические устройства

24. К программно-техническим мерам защиты информации относятся:
a) электронные устройства и специальные программы, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты
b) меры организационного характера
c) всевозможные нормы поведения, которые традиционно сложились в обществе
d) разного рода механические, электрические и электронно-механические устройства

25. Что такое учетная запись:
a) Запись, содержащая все сведения, определяющие пользователя в ОС
b) совокупность массивов информации, систем кодирования и классификации информации
c) совокупность программных средств и программных документов, необходимых при их эксплуатации
d) Сведения, определяющих меру наших знаний об объекте

26. Типы учетных записей:
a) Только администратор
b) Администратор, учетная запись с ограниченными правами, гость.
c) Только администратор и учетная запись с ограниченными правами
d) только учетная запись с ограниченными правами и гость.

27. Код Хэмминга представляет:
a) содержание
b) точность
c) блочный код, который позволяет выявить и исправить ошибочно переданный бит, в пределах переданного блока.
d) информативность

28. Код Хафмана создает:
    a) пространственные и атрибутивные данные
    b) целочисленные типы данных
    c) структурированные файлы
    d) файл меньших размеров из исходного

29. Электронная цифровая подпись это:
    a) математическиЙ алгоритм
    b) **реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки.**
    c) сведения, которые характеризуют местоположение объектов в пространстве относительно друг друга
    d) это качественные или количественные характеристики пространственных объектов

30. ЭЦП формируется при помощи:
    a) Электронного документа
    b) Математических алгоритмов
    c) некого «закрытого ключа»
    d) математических алгоритмов на основе собственно документа и некого «закрытого ключа»

31. Электронная подпись позволяет:
    a) проверять целостность данных
    b) обеспечивает конфиденциальность данных
    c) передавать скрытую информацию
    d) сжимать информацию

32. Криптография это:
    a) дисциплина, изучающая кодирование
    b) **наука об обеспечении безопасности данных**
    c) наука об конфиденциальности
    d) сведения о фактах и явлениях происходящих в обществе

33. Шифрование это:
    a) Одномерные данные имеющие одну размерность – длину
    b) обеспечение конфиденциальности данных
    c) преобразование данных в сжатый вид
    d) преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки

34. Криптография не занимается решение проблемы:
    a) конфиденциальности
    b) аутентификации
    c) секретности
    d) контроля участников взаимодействия

    .

35. Виды шифрования:

a) Секретное и доступное
b) внешнее и внутренне
c) открытое и закрытое
d) Симметричное и ассиметричное

36. Шифрование данных осуществляет:

a) получатель
b) отправитель
c) криптоаналитик
d) злоумышленник

37. Злоумыгленник – это:

a) Лицо, преднамеренно реализующие угрозы
b) Лица, случайно реализующие угрозы
c) Лицо, выполняющее кодирование информации
d) Лицо, выполняющее шифрование информации

38. Аутентификация это:

a) дешифрование
b) шифрование
c) проверка подлинности
d) распознавание

39. Аутентификация это:

a) распознавание
b) дешифрование
c) шифрование
d) проверка подлинности

Ответы:

1. a	2. b	3. a	4. d	5. b
6. a	7. c	8. b	9. a	10. b
11. b,c	12. a,b	13. d	14. a	15. b
16. a	17. d	18. c	19. a	20. c
21. b	22. b	23. d	24. d	25. a
26. a	27. b	28. c	29. d	30. b
31. d	32. a	33. b	34. d	35. c
36. d	37. b	38. a	39. c	40. a

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Рекомендуемая литература и источники информации

№	Виды занятий (лк, пз, лб, срс, ирс)	Комплект необходимой учебной литературы по дисциплинам (наименование учебника, учебного пособия, конспект лекций, учебно-методической литературы)	Автор	Издат. и год издания	Кол-во пособий, учебников и прочей литературы	
					в библиотеке	на кафедре
Основная литература						
1.	ЛК,СР, КР	Информационная безопасность и защита информации. Учебное пособие для ВУЗов.	Мельников В.П., Клейменов С.А., Петраков А.М.	М.: Академия, 2007г.-336с., ил. ISBN 978-5-7695-4884-0	47	
2.	ЛК,СР, КР	Инженерно-техническая защита информации [Электронный ресурс]	Рагозин Ю. Н.	СПб.: Интермедия, 2018. — 168 c. — 978-5-4383-0161-5.	http://www.iprbookshop.ru/73641.html	
3.	ЛК,СР, КР	Организационная защита информации [Электронный ресурс]	Аверченков В. И.	Брянск: Брянский государственный технический университет, 2012. — 184 c. — 978-89838-489-0	http://www.iprbookshop.ru/7002.html	
4.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. — 95 c. — 2227-8397	http://www.iprbookshop.ru/17925.html	
5.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. — 104 c. — 2227-8397	http://www.iprbookshop.ru/17926.html	

6.	ЛК,СР, КР	Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие	Креопалов В. В.	М.: Евразийский открытый институт, 2011. — 278 с. — 978-5-374-00507-3.	http://www.iprbookshop.ru/10871.html
7.	ЛК,СР, КР	Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие	Башлы П. Н.	М.: Евразийский открытый институт, 2012. — 311 с. — 978-5-374-00301-7.	http://www.iprbookshop.ru/10677.html
8.	ЛК,СР, КР	Методы и средства криптографической защиты информации [Электронный ресурс] :	Алексеев В. А.	Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009. — 16 с. — 2227-8397.	
http://www.iprbookshop.ru/17710.html					
9.	ЛК,СР, КР	Комплексная защита информации в компьютерных системах. Учебное пособие	Завгородний В.И.	М.: Логос, Пбоюл Н.А.Егоров, 2001-264с.,	http://www.iprbookshop.ru/16510.html
10.	ЛК,СР, КР	Методы и средства защиты информации в компьютерных системах. Учебное пособие для ВУЗов.3-е издание	Хорев П.Б.	М.: Академия, 2007-256.: ил.-(высш.проф. образ.) ISBN 978-5-7695-4157-5	http://www.iprbookshop.ru/1723.html
11.	ЛК,СР, КР	Организационное обеспечение информационной безопасности. Учебник для ВУЗов.	Романов О.А., Бабин С.А., Жданов С.Г.	М.: Академия, 2008-190с. ISBN 978-5-7695-4272-5	http://www.iprbookshop.ru/17760.html
12.	ЛК,СР, КР	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. Учебное пособие для ВУЗов	Белкин П.Б., Михальский О.О., Першаков А.С. и др.	М.: Радио и связь, 1999.-168с.	http://www.iprbookshop.ru/17380.html
13.	ЛК,СР, КР	Основы криптографии. Учебное пособие – 2.е издание.		М.: Гелиос АРВ; 2002.-480с., ил.	http://www.iprbookshop.ru/17729.html
14.	ЛК,СР, КР	Криптография: скоростные шифры	Молдовян А.А. и др.	СПб., БХВ-Петербург, 2002.-496с.	http://www.iprbookshop.ru/17010.html
Интернет - источники					
15.	ЛК,СР, КР	http://dstu.ru/nauka/biblioteka/ – образовательный портал университета			

16.	ЛК,СР, КР	http://www.elibrary.ru – научная электронная библиотека
17.	ЛК,СР, КР	http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.

Базы данных, информационно – справочные и поисковые системы; вузовские электронно-библиотечные системы учебной литературы.

Материально-техническое обеспечение дисциплины: компьютерный класс для выполнения лабораторного практикума с использованием интегрированной среды разработки программ.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО по направлению 38.03.01 Экономика.

Рецензент от выпускающей кафедры (работодателя) по направлению

_____

Подпись ФИО

Дополнения и изменения в рабочей программе
на 20__/___ учебный год

В рабочую программу вносятся следующие изменения

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Рабочая программа пересмотрена и одобрена на заседании кафедры _____20

Заведующий кафедрой _____

Внесенные изменения утверждаю
Проректор
по учебной работе _____

(декан) _____