

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАТАРСТАН

Государственное бюджетное образовательное учреждение
высшего образования
«Альметьевский государственный нефтяной институт»



УТВЕРЖДАЮ
Первый проректор АГНИ
Иванов А.Ф.
« 25 » 06 2018г.

Рабочая программа дисциплины Б1.В.ДВ.06.02

ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки: 38.03.01 – «Экономика»

Направленность (профиль) программы: «Экономика предприятий и организаций»

Квалификация выпускника: бакалавр

Форма обучения: очная, заочная

Язык обучения: русский

Год начала обучения по образовательной программе: 2018

Статус	ФИО	Подпись	Дата
Автор	О.Н.Потапова		4.06.2018
Рецензент	Л.М. Садриева		5.06.2018
Зав. обеспечивающей кафедрой математики и информатики	З.Ф. Зарипова		6.06.2018

Согласовано:

Зав. выпускающей кафедрой экономики и управления предприятием	Р.Ш.Садыкова		22.06.2018
---	--------------	--	------------

Альметьевск, 2018г.

Содержание

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования
3. Объем дисциплины в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
 - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине
 - 4.2. Содержание дисциплины
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине
6. Фонд оценочных средств по дисциплине
 - 6.1. Перечень оценочных средств
 - 6.2. Уровень освоения компетенций и критерии оценивания результатов обучения
 - 6.3. Варианты оценочных средств
 - 6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций
7. Перечень основной, дополнительной учебной литературы и учебно-методических изданий, необходимых для освоения дисциплины
8. Перечень профессиональных баз данных, информационных справочных систем и информационных ресурсов, необходимых для освоения дисциплины
9. Методические указания для обучающихся по освоению дисциплины
10. Перечень программного обеспечения
11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине
12. Средства адаптации преподавания дисциплины к потребностям обучающихся лиц с ограниченными возможностями здоровья

ПРИЛОЖЕНИЯ

- Приложение 1. Аннотация рабочей программы дисциплины
Приложение 2. Лист внесения изменений
Приложение 3. Фонд оценочных средств

Программа дисциплины «Защита информации» разработана старшим преподавателем кафедры математики и информатики **Потаповой О.Н.**

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

Компетенции обучающегося формируемые в результате освоения дисциплины «Защита информации»:

Оцениваемые компетенции (код, наименование)	Результаты освоения компетенции	Оценочные средства текущего контроля и промежуточной аттестации
<p>ОПК-1 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p>Знать: -основы системы информационной и библиографической культуры; -основы информационно-коммуникационных технологий; -основные требования информационной безопасности при решении задач профессиональной деятельности. Уметь: -анализировать библиографический и информационный материал используя информационно - коммуникационные технологии; -определять стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности. Владеть: -навыками анализа профессионально-практической деятельности работы с использованием основных требований информационной безопасности с применением информационно-коммуникационных технологий.</p>	<p>Текущий контроль: Компьютерное тестирование по темам 1- 9 Лабораторные работы по темам 3-6, 8, 9</p> <p>Промежуточная аттестация: 1 семестр Зачет 2 семестр Экзамен</p>
<p>ПК-10 Способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии</p>	<p>Знать: - основные методы решения коммуникативных задач; - специфику различных способов решения коммуникативных задач; - современные технические средства и информационные технологии, используемые при решении коммуникативных задач;</p>	<p>Текущий контроль: Компьютерное тестирование по темам 1- 9 Лабораторные работы по темам 3-6, 8, 9</p> <p>Промежуточная аттестация: 1 семестр Зачет 2 семестр Экзамен</p>

	<p>Уметь:</p> <ul style="list-style-type: none"> - пользоваться современными техническими средствами и информационными технологиями при решении коммуникативных задач. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками для самостоятельного, методически правильного решения коммуникативных задач; - техническими средствами и информационными технологиями при решении коммуникативных задач. 	
--	--	--

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Дисциплина «Защита информации» является дисциплиной по выбору, входит в состав Блока 1 «Дисциплины (модули)» и относится к вариативной части ОПОП по направлению подготовки 38.03.01 – «Экономика», направленность (профиль) программы – «Экономика предприятий и организаций» - «Б1.В.ДВ.06.02».

Дисциплина изучается на 1 курсе в 1 и 2 семестрах¹/на 1 курсе в 1 семестре².

3. Объем дисциплины в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов.

Контактная работа обучающихся с преподавателем 94ч¹/22 ч²:

- лекции 36ч¹/8ч².;
- лабораторные работы 54ч¹/8 ч².;
- КСР 4ч¹/6ч².

Самостоятельная работа 86ч¹/185 ч².

Форма промежуточной аттестации дисциплины: зачет в 1 семестре, экзамен во 2 семестре¹/ зачет и экзамен на 1 курсе².

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине

¹ Очная форма обучения

² Заочная форма обучения

Тематический план дисциплины

Очная форма обучения

№ п/п	Темы 6	семестр	Виды и часы контактной работы, их трудоемкость (в ч)				Самостоятельная работа
			Лекции	практические занятия	лабораторные работы	КСР	
1	Основные понятия и определения в области информационной безопасности. Концептуальная модель информационной безопасности	1	2	-	-	-	5
2	Исследование причин нарушений безопасности.	1	2	-	-	1	10
3	Ассиметричные системы шифрования.	1	2		12	1	10
4	Традиционное шифрование: классические методы. Криптостойкость.	1	8	-	16	-	5
5	Хэш-функции и аутентификация сообщений.	1	4	-	8	-	4
Итого за семестр		1	18		36	2	34
6	Алгоритмы генерации псевдослучайных последовательностей чисел.	2	4	-	10	1	15
7	Архитектура защищенных операционных систем.	2	4	-	-	1	15
8	Электронная цифровая подпись.	2	4		2	-	10
9	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.	2	6	-	6	-	12
Итого за семестр		2	18	-	18	2	52
Итого по дисциплине			36	-	54	4	86

Заочная форма обучения

№ п/п	Темы 6	курс	Виды и часы контактной работы, их трудоемкость (в ч)				Самостоятельная работа
			Лекции	практические занятия	лабораторные работы	КСР	
1	Основные понятия и определения в области информационной	1	1	-	-	-	25

	безопасности. Концептуальная модель информационной безопасности						
2	Исследование причин нарушений безопасности.	1	1	-	-	-	30
3	Ассиметричные системы шифрования.	1	1		4	3	20
4	Традиционное шифрование: классические методы. Криптостойкость.	1	1	-	4	3	30
5	Хэш-функции и аутентификация сообщений.	1	1	-	-	-	20
6	Алгоритмы генерации псевдослучайных последовательностей чисел.	1	1	-	-	-	20
7	Архитектура защищенных операционных систем.	1	2	-	-	-	15
8	Электронная цифровая подпись.	1	-		-	-	10
9	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.	1	-	-	-	-	15
Итого по дисциплине			8	-		6	185

4.2 Содержание дисциплины

Тема	Кол-во часов	Используемый метод	Формируемые компетенции
Дисциплинарный модуль 1.1.			
Тема 1. Основные понятия и определения в области информационной безопасности. Концептуальная модель информационной безопасности. – 2ч.			
<u>Лекция 1.</u> Информационная безопасность. Атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.	2	-	ОПК-1 ПК-10
Тема 2. Исследование причин нарушений безопасности.- 2ч.			
<u>Лекция 2.</u> Причины нарушения информационной безопасности. Способы предотвращения нарушений информационной безопасности.	2		ОПК-1 ПК-10
Тема 3. Ассиметричные системы шифрования. – 14ч.			
<u>Лекция 3.</u> Понятия однонаправленной функции и однонаправленной функции с лазейкой.	2		ОПК-1 ПК-10

Тема	Кол-во часов	Используемый метод	Формируемые компетенции
Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамала. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.			
Лабораторное занятие 1-2. Алгоритм RSA	4	<i>ситуационный анализ</i>	ОПК-1 ПК-10
Лабораторное занятие 3-4. Алгоритм DSA	4		ОПК-1 ПК-10
Лабораторное занятие 5-6. Схема Эль-Гамала.	4	<i>групповое обсуждение</i>	ОПК-1 ПК-10
Дисциплинарный модуль 1.2.			
Тема 4. Традиционное шифрование: классические методы. – 24ч.			
Лекция 4. Основные понятия и определения. Подстановочные и перестановочные шифры.	2	-	ОПК-1 ПК-10
Лекция 5. Шифры Цезаря, Виженера, Вернама.	2		ОПК-1 ПК-10
Лекция 6. Дисковые шифраторы. Исследования Шеннона в области криптографии.	2		ОПК-1 ПК-10
Лекция 7. Нераскрываемость шифра Вернама.	2		ОПК-1 ПК-10
Лабораторное занятие 7-8. Простая и двойная перестановки.	4	<i>групповое обсуждение</i>	ОПК-1 ПК-10
Лабораторное занятие 9-10. Одиночная перестановка по ключу.	4		ОПК-1 ПК-10
Лабораторное занятие 11-12. Шифр Цезаря.	4	<i>работа в малых группах</i>	ОПК-1 ПК-10
Лабораторное занятие 13-14. Шифр Виженера. Шифр Вернама.	4	<i>групповое обсуждение</i>	ОПК-1 ПК-10
Тема 5. Хэш-функции и аутентификация сообщений. – 12ч.			
Лекция 8. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411.	2		ОПК-1 ПК-10
Лекция 9. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.	2		ОПК-1 ПК-10
Лабораторное занятие 15-16. Хэш-функция MD5.	4	<i>работа в малых группах</i>	ОПК-1 ПК-10
Лабораторное занятие 17-18. Хэш-функция SHA.	4	<i>работа в малых группах</i>	ОПК-1 ПК-10
2 семестр			
Дисциплинарный модуль 2.1.			
Тема 6. Алгоритмы генерации псевдослучайных последовательностей чисел. – 14ч.			
Лекция 10. Различные способы создания псевдослучайных чисел.	2		ОПК-1 ПК-10

Тема	Кол-во часов	Используемый метод	Формируемые компетенции
Лекция 11. Различные способы создания псевдослучайных чисел.	2		ОПК-1 ПК-10
Лабораторное занятие 19. Линейный конгруэнтный метод генерации псевдослучайных чисел	2	<i>ситуационный анализ</i>	ОПК-1 ПК-10
Лабораторное занятие 20-21. Алгоритм Блюма-Блюма-Шума.	4		ОПК-1 ПК-10
Лабораторное занятие 22-23. Алгоритм xor-shift. Тестирование по модулю 2.1	4	<i>работа в малых группах</i>	ОПК-1 ПК-10
Тема 7. Архитектура защищенных операционных систем. – 4ч.			
Лекция 12-13. Защищенная операционная система. Идентификация, аутентификация, разграничение доступа, протоколирование, аудит, экранирование, туннелирование, шифрование.	4		ОПК-1 ПК-10
Дисциплинарный модуль 2.2.			
Тема 8. Электронная цифровая подпись. – 6ч.			
Лекция 14. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись	2		ОПК-1 ПК-10
Лекция 15. Стандарты цифровой подписи ГОСТ 3410 и DSS.	2		ОПК-1 ПК-10
Лабораторное занятие 24. Стандарт цифровой подписи DSS. Генерация цифровой подписи.	2	<i>работа в малых группах</i>	ОПК-1 ПК-10
Тема 9. Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. - 12ч.			
Лекция 16. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext.	2	<i>групповое обсуждение</i>	ОПК-1 ПК-10
Лекция 17. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля.	2		ОПК-1 ПК-10
Лекция 18. Описание алгоритмов DES и тройного DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения.	2		ОПК-1 ПК-10
Лабораторное занятие 25-26. Изучение американского стандарта шифрования данных DES.	4	<i>работа в малых группах</i>	ОПК-1 ПК-10
Лабораторное занятие 27. Изучение отечественного стандарта шифрования данных ГОСТ 28147-89. Тестирование по модулю 2.2	2	<i>работа в малых группах</i>	ОПК-1 ПК-10

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающихся выполняется по заданию преподавателя, без его непосредственного участия и направлена на самостоятельное изучение отдельных аспектов тем дисциплины.

Цель самостоятельной работы – подготовка современного компетентного специалиста и формирования способной и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Самостоятельная работа способствует формированию аналитического и творческого мышления, совершенствует способы организации исследовательской деятельности, воспитывает целеустремленность, систематичность и последовательность в работе студентов, развивает у них навык завершать начатую работу.

Виды самостоятельной работы студентов:

- изучение понятийного аппарата дисциплины;
- проработка тем дисциплины;
- работа с основной и дополнительной литературой;
- самоподготовка к лабораторным занятиям;
- подготовка к промежуточной аттестации;
- работа в библиотеке;
- изучение сайтов по теме дисциплины в сети Интернет с целью подготовки докладов и презентаций;

Темы для самостоятельной работы обучающегося, порядок их контроля по дисциплине «Защита информации» приведены в методических указаниях:

Потапова О.Н. Защита информации: методические указания по выполнению лабораторных работ и организации самостоятельной работы по дисциплине «Защита информации» для бакалавров направления подготовки 38.03.01 «Экономика» очной и заочной формы обучения. - Альметьевск: тип. АГНИ, 2016г.

6. Фонд оценочных средств по дисциплине

Основной целью формирования ФОС по дисциплине «Защита информации» является создание материалов для оценки качества подготовки обучающихся и установления уровня освоения компетенций.

Полный перечень оценочных средств текущего контроля и промежуточной аттестации по дисциплине приведен в Фонде оценочных средств (приложение 3 к данной рабочей программе).

Текущий контроль освоения компетенций по дисциплине проводится при изучении теоретического материала, выполнении лабораторных работ.

Итоговой оценкой освоения компетенций является промежуточная аттестация в форме экзамена и зачета, проводимая с учетом результатов текущего контроля.

6.1. Перечень оценочных средств по дисциплине «Информационные технологии»

Этапы формирования компетенций	Вид оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Текущий контроль			
1	Лабораторная работа	Может выполняться в индивидуальном порядке или группой обучающихся. Задания в лабораторных работах должны включать элемент командной работы. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания	Темы, задания для выполнения лабораторных работ

		в процессе решения практических задач и оценить уровень сформированности аналитических, исследовательских навыков, а также навыков практического мышления. Позволяет оценить способность к профессиональным трудовым действиям	
2	Тестирование компьютерное	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося по соответствующим компетенциям. Обработка результатов тестирования на компьютере обеспечивается специальными программами. Позволяет проводить самоконтроль (репетиционное тестирование), может выступать в роли тренажера при подготовке к зачету или экзамену	Фонд тестовых заданий
Промежуточная аттестация			
3	Зачет	Итоговая форма оценки степени освоения дисциплины. Зачет направлен на выявление соответствия усвоенного материала дисциплины требованиям рабочей программы дисциплины. Зачет выставляется по результатам текущего контроля без дополнительного опроса.	
4	Экзамен	Итоговая форма определения степени достижения запланированных результатов обучения (оценивания уровня освоения компетенций). Экзамен проводится в устной форме или в форме компьютерного тестирования по всем темам дисциплины.	Перечень вопросов и задач к экзамену

6.2. Уровень освоения компетенции и критерии оценивания результатов обучения

№ п/п	Оцениваемые компетенции (код, наименование)	Планируемые результаты обучения	Уровень освоения компетенций			
			Продвинутый уровень	Средний уровень	Базовый уровень	Компетенции не освоены
			Критерии оценивания результатов обучения			
			«отлично» (от 86 до 100 баллов)	«хорошо» (от 71 до 85 баллов)	«удовлетворительно» (от 55 до 70 баллов)	«неудовлетв.» (менее 55 баллов)
			Зачтено (от 35 до 60 баллов)			Не зачтено (менее 35 баллов)
1	ОПК-1 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: -основы системы информационной и библиографической культуры; -основы информационно-коммуникационных технологий; -основные требования информационной безопасности при решении задач профессиональной деятельности.	Знает на высоком уровне: современные информационные технологии, основы функционирования глобальных информационно-коммуникационных сетей и баз данных	Знает: современные информационные технологии, основы функционирования глобальных информационно-коммуникационных сетей и баз данных	Частично знает: современные информационные технологии, основы функционирования глобальных информационно-коммуникационных сетей и баз данных	Не знает: современные информационные технологии, основы функционирования глобальных информационно-коммуникационных сетей и баз данных
		Уметь: -анализировать библиографический и информационный материал используя информационно - коммуникационные технологии; -определять стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности.	Умеет на высоком уровне: вести поиск информации в глобальных компьютерных сетях, осуществлять выбор инструментальных средств для обработки аналитических данных в соответствии с поставленной задачей, анализировать результаты расчетов и обосновывать полученные выводы	Умеет: вести поиск информации в глобальных компьютерных сетях, осуществлять выбор инструментальных средств для обработки аналитических данных в соответствии с поставленной задачей, анализировать результаты расчетов и обосновывать полученные выводы	Частично умеет: вести поиск информации в глобальных компьютерных сетях, осуществлять выбор инструментальных средств для обработки аналитических данных в соответствии с поставленной задачей, анализировать результаты расчетов и обосновывать полученные выводы	Не умеет: вести поиск информации в глобальных компьютерных сетях, осуществлять выбор инструментальных средств для обработки аналитических данных в соответствии с поставленной задачей, анализировать результаты расчетов и обосновывать полученные выводы

		<p>Владеть: -навыками анализа профессионально-практической деятельности работы с использованием основных требований информационной безопасности с применением информационно-коммуникационных технологий.</p>	<p>Владеет на высоком уровне навыками использования компьютерных технологий как средства управления информацией, использования информации, полученной из глобальной сети Интернет</p>	<p>Владеет: навыками использования компьютерных технологий как средства управления информацией, использования информации, полученной из глобальной сети Интернет</p>	<p>Частично владеет навыками использования компьютерных технологий как средства управления информацией, использования информации, полученной из глобальной сети Интернет</p>	<p>Не владеет: навыками использования компьютерных технологий как средства управления информацией, использования информации, полученной из глобальной сети Интернет</p>
2	<p>ПК-10 Способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии</p>	<p>Знать: - основные методы решения коммуникативных задач; - специфику различных способов решения коммуникативных задач; - современные технические средства и информационные технологии, используемые при решении коммуникативных задач</p>	<p>Знает на высоком уровне: современные технические средства, информационные технологии для решения коммуникативных задач</p>	<p>Знает: современные технические средства, информационные технологии для решения коммуникативных задач</p>	<p>Частично знает: современные технические средства, информационные технологии для решения коммуникативных задач</p>	<p>Не знает: современные технические средства, информационные технологии для решения коммуникативных задач</p>
		<p>Уметь: - пользоваться современными техническими средствами и информационными технологиями при решении коммуникативных задач</p>	<p>Умеет на высоком уровне: решать коммуникативные задачи с применением соответствующих информационных технологий и технических средств</p>	<p>Умеет: решать коммуникативные задачи с применением соответствующих информационных технологий и технических средств</p>	<p>Частично умеет: решать коммуникативные задачи с применением соответствующих информационных технологий и технических средств</p>	<p>Не умеет: решать коммуникативные задачи с применением соответствующих информационных технологий и технических средств</p>

		<p>Владеть:</p> <ul style="list-style-type: none"> - навыками для самостоятельного, методически правильного решения коммуникативных задач; - техническими средствами и информационными технологиями при решении коммуникативных задач. 	<p>Владеет на высоком навыками работы с компьютерными и информационными технологиями, необходимыми для решения коммуникативных задач</p>	<p>Владеет: навыками работы с компьютерными и информационными технологиями, необходимыми для решения коммуникативных задач</p>	<p>Частично владеет: навыками работы с компьютерными и информационными технологиями, необходимыми для решения коммуникативных задач</p>	<p>Не владеет: навыками работы с компьютерными и информационными технологиями, необходимыми для решения коммуникативных задач</p>
--	--	---	--	--	---	---

6.3. Варианты оценочных средств

6.3.1. Тестирование компьютерное

6.3.1.1 Порядок проведения

Тестирование компьютерное по дисциплине «Защита информации» проводится два раза в течение семестра. Банк тестовых заданий содержит список вопросов и различные варианты ответов.

6.3.1.2 Критерии тестирования

Результат теста зависит от количества вопросов, на которые был дан правильный ответ.

6.3.1.3 Содержание оценочного средства

Тестовые задания для оценки уровня сформированности компетенций

Код компетенции	Тестовые вопросы	Варианты ответов			
		1	2	3	4
Дисциплинарный модуль 1.1.					
ОПК-1 ПК-10	Какие операционные системы являются наиболее распространенными в настоящее время	Семейства windows	Класса Unix	Реального времени	
	Назовите компоненты операционной системы	Ядро	Загрузчик	Интерпретатор	Драйверы устройств
	В каком году была разработана первая Unix-система	1969г.	1968г.	1955г.	1981г.
	Какой из компонентов не входит в системное программное обеспечение	Операционная система	Дополнительное системное ПО	Пользовательский интерфейс	Встроенное программное обеспечение
	В чем файловая система ext2 превосходит ext3?	Выше скорость чтения-записи	Меньше размер кластера	Поддерживает жесткие диски размером больше 2Тб	Журналируемая
Дисциплинарный модуль 1.2.					
ОПК-1 ПК-10	При полномочной политике безопасности совокупность меток с одинаковыми значениями образует	область равной критичности	область равного доступа	уровень безопасности	уровень доступности
	Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о	аудит	аутентификация	авторизация	идентификация

	предоставлении ему доступа к ресурсам системы — это				
	С помощью закрытого ключа информация	копируется	транслируется	расшифровывается	зашифровывается
	Конкретизацией модели Белла-ЛаПадула является модель политики безопасности	LWM	На основе анализа угроз	Лендвера	С полным перекрытием
	Какая из этих настроек не входит в состав BIOS материнских плат	Установка времени системных часов, даты календаря	Загрузка с сетевой платы по технологии PXE	Настройка периферии, не приспособленной к работе в режиме «plugandplay».	Отключение некоторых тестов, что ускоряет загрузку ОС.
Дисциплинарный модуль 2.1.					
ОПК-1 ПК-10	Наименее затратный криптоанализ для криптоалгоритма DES	перебор по выборочному ключевому пространству	разложение числа на сложные множители	перебор по всему ключевому пространству	разложение числа на простые множители
	Недостаток систем шифрования с открытым ключом	при использовании простой замены легко произвести подмену одного зашифрованного текста другим	относительно низкая производительность	необходимость распространения секретных ключей	на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки зашифрованного текста
	Наименее затратный криптоанализ для криптоалгоритма RSA	перебор по выборочному ключевому пространству	разложение числа на сложные множители	перебор по всему ключевому пространству	разложение числа на простые множители
	Длина исходного ключа в ГОСТ 28147-89 (бит)	256	64	128	56
	Главным параметром криптосистемы является показатель	скорости шифрования	безошибочности шифрования	надежности функционирования	криптостойкости
Дисциплинарный модуль 2.2.					
ОПК-1 ПК-10	Шифрование методом перестановки:	символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста	символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности	шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор	символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
	Символы шифруемого	гаммирования	подстановки	кодирования	перестановки

	текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод				
	Шифр DES это	система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки	система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители	блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны	шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами
	Шифр ГОСТ 28147-89 это	система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки	система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители	блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны	шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами
	Система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки – это шифр	IDEA	RSA	ГОСТ 28147-89	DES

6.3.2. Лабораторные работы

6.3.2.1 Порядок проведения

Лабораторные работы выполняются обучающимися самостоятельно во время аудиторных занятий. Трудоемкость лабораторных работ в часах приведена в рабочей программе дисциплины, см. п. 4.2.

По завершению лабораторных работ студент должен продемонстрировать знание методики выполнения работы, уметь интерпретировать полученные результаты. Максимальный балл выставляется обучающемуся, если работа выполнена в срок.

6.3.2.2. Критерии оценивания

Баллы в интервале 86-100% от максимальных ставятся (максимальный балл по каждой лабораторной работе приведен в п. 6.4), если обучающимся:

- оборудование и методы использованы правильно, проявлена продвинутая теоретическая подготовка, необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует ее целям.

Баллы в интервале 71-85% от максимальных ставятся, если обучающимся:

- оборудование и методы использованы в основном правильно, проявлена средняя теоретическая подготовка, необходимые навыки и умения в основном освоены, результат лабораторной работы в основном соответствует ее целям.

Баллы в интервале 55-70% от максимальных ставятся, если обучающийся:

- оборудование и методы частично использованы правильно, проявлена базовая теоретическая подготовка, необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует ее целям.

Баллы в интервале 0-54% от максимальных ставятся, если обучающимся:

- оборудование и методы использованы неправильно, проявлена неудовлетворительная теоретическая подготовка, необходимые навыки и умения не освоены, результат лабораторной работы не соответствует её целям.

6.3.2.3. Содержание оценочного средства

Задания к лабораторным занятиям:

Лабораторная работа №1-2. Алгоритм RSA.

Задание (ОПК-1, ПК-10):

Выполнить упражнения:

1. Вычисление ключей.
2. Шифрование.
3. Расшифрование.

Основные теоретические положения, последовательность выполнения работы, методика, правила оформления и варианты индивидуальных заданий по лабораторным работам описаны в методических указаниях:

Потапова О.Н. Защита информации: методические указания по выполнению лабораторных работ и организации самостоятельной работы по дисциплине «Защита информации» для бакалавров направления подготовки 38.03.01 «Экономика» всех форм обучения. - Альметьевск: тип. АГНИ, 2016г.

6.3.4. Экзамен

6.3.4.1. Порядок проведения

Тип задания – вопросы к экзамену, практическая часть. Вопросы к экзамену выдаются студентам заранее. Практическая часть основана на пройденном материале на лабораторных занятиях. Студент должен дать полный, развернутый и обоснованный ответ на соответствующий вопрос в устной форме, выполнить практическую часть. Билет на экзамен включает один теоретический вопрос и одно практическое задание. Ответ обучающегося оценивается преподавателем в соответствии с установленными критериями.

На экзамене, который проводится в форме компьютерного тестирования, студенту предоставляется блок тестовых заданий, которые генерируются

автоматической тестирующей системой персонально в случайном порядке и содержат вопросы по всему перечню тем дисциплины. Кроме того, студенту предоставляется одно практическое задание, которое необходимо выполнить за компьютером.

6.3.4.2. Критерии оценивания

Баллы в интервале 86-100% от максимальных ставятся, если обучающийся:

- демонстрирует продвинутый уровень владения знаниями, умениями и навыками соответствующих компетенций;
- проявил высокую эрудицию и свободное владение материалом дисциплины;
- дал ответы на вопросы четкие, обоснованные и полные, проявил готовность к дискуссии.

Баллы в интервале 71-85% от максимальных ставятся, если обучающийся:

- демонстрирует знания, умения, навыки, сформированные на среднем уровне соответствующих компетенций;
- способен самостоятельно воспроизводить и применять соответствующие знания, умения и навыки для решения типовых задач дисциплины;
- дал ответы на вопросы преимущественно правильные, но недостаточно четкие.

Баллы в интервале 55-70% от максимальных ставятся, если обучающийся:

- демонстрирует знания, умения, навыки, сформированные на базовом уровне соответствующих компетенций;
- частично, с помощью извне (например, с использованием наводящих вопросов) может воспроизводить и применять соответствующие знания, умения, навыки;
- дал ответы на вопросы не полные.

Баллы в интервале 0-54% от максимальных ставятся, если обучающийся:

- не ответил на большую часть вопросов;
- демонстрирует полную некомпетентность в материале дисциплины, не способен самостоятельно, без помощи извне, воспроизводить и применять соответствующие знания, умения, навыки.

6.3.4.3. Содержание оценочного средства

Примерные вопросы к экзамену:

№ п/п	Наименование вопроса	ОПК-1	ПК-10
1.	Понятие информационной безопасности. Основные составляющие. Важность проблемы.	+	
2.	Распространение объектно-ориентированного подхода на информационную безопасность.	+	
3.	Понятие угрозы. Наиболее распространенные угрозы. 4. Классификация угроз.	+	
4.	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	+	
5.	Законодательный уровень информационной безопасности.	+	
6.	Обзор зарубежного законодательства в области ИБ. Назначение и задачи в сфере обеспечения информационной безопасности.	+	+
7.	Международные стандарты информационного обмена.	+	+
8.	Стандарт ISO/IEC15408.	+	+

9.	Российские стандарты защищенности автоматизированных систем.	+	+
10.	Основные положения теории информационной безопасности.	+	+
11.	Модели безопасности и их применение.	+	+
12.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	+	+
13.	Информационная безопасность в условиях функционирования в России глобальных сетей.	+	+
14.	Виды противников или "нарушителей". Понятия о видах вирусов	+	+
15.	Виды возможных нарушений информационной системы. Виды защиты.	+	+
16.	Файловые вирусы. Загрузочные вирусы.	+	+
17.	Вирусы и операционные системы. Методы и средства борьбы с вирусами.	+	+
18.	Профилактика заражения вирусами компьютерных систем.	+	
19.	Защита информации от случайных угроз.	+	+
20.	Дублирование информации.	+	+
21.	Повышение надежности компьютерных систем.	+	+
22.	Обеспечение отказоустойчивости компьютерных систем.	+	+
23.	Блокировка ошибочных операций.	+	+
24.	Защита информации от традиционного шпионажа и диверсий.	+	+
25.	Система охраны объектов компьютерных систем.	+	+
26.	Организация работы с конфиденциальными информационными ресурсами.	+	+
27.	Противодействие подслушиванию и наблюдению в оптическом диапазоне.	+	+
28.	Средства борьбы с закладными подслушивающими устройствами.	+	+
29.	Защита от злоумышленных действий обслуживающего персонала и пользователей.	+	+
30.	Средства защиты компьютеров. Программно - аппаратные методы и средства ограничения доступа к компонентам компьютера.	+	+
31.	Типы несанкционированного доступа и условия работы средств защиты.	+	+
32.	Анализ способов нарушений информационной безопасности.	+	+
33.	Использование защищенных компьютерных систем.	+	+
34.	Защита от несанкционированного копирования программного обеспечения.	+	+
35.	Методы криптографии. Основные понятия шифрования.	+	+
36.	Методы шифрования с симметричным ключом.	+	+
37.	Системы шифрования с открытым ключом.	+	
38.	Стандарты шифрования.		+
39.	Промышленные программные средства Kerberos.		+
40.	Промышленные программные средства PGP.		+
41.	Методы и средства хранения ключевой информации.		+
42.	Анализ программных реализаций.		+
43.	Защита от разрушающих программных воздействий.		+
44.	Основные технологии построения защищенных ЭИС.		+

45.	Системные вопросы защиты программ и данных.		+
46.	Электронная цифровая подпись.		+
47.	Критерии защищенности компьютерных систем.		+
48.	Идентификация и аутентификация.		+

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

В ГБОУ ВО АГНИ действует балльно-рейтинговая система оценки знаний обучающихся.

Общие положения:

- Для допуска к экзамену студенту необходимо набрать не менее **35 баллов** по результатам текущего контроля знаний.

- Если студент по результатам текущего контроля в учебном семестре набрал от **55** до **60** баллов и по данной дисциплине предусмотрен экзамен, то по желанию студента в экзаменационную ведомость и зачетную книжку экзаменатором без дополнительного опроса может быть проставлена оценка «удовлетворительно».

- Выполнение тестов принимается в установленные сроки.

- Защита лабораторных работ принимается в установленные сроки.

- При наличии уважительных причин срок сдачи может быть продлен, но не более чем на две недели.

- Рейтинговая оценка регулярно доводится до студентов и передается в деканат в установленные сроки.

Порядок выставления рейтинговой оценки:

1. До начала семестра преподаватель формирует рейтинговую систему оценки знаний студентов по дисциплине, с разбивкой по текущим аттестациям.

2. Преподаватель обязан на первом занятии довести до сведения студентов условия рейтинговой системы оценивания знаний и умений по дисциплине.

3. После проведения контрольных испытаний преподаватель обязан ознакомить студентов с их результатами и по просьбе студентов объяснить объективность выставленной оценки.

4. В случае пропусков занятий по неуважительной причине студент имеет право добрать баллы после изучения всех модулей до начала экзаменационной сессии.

5. Студент имеет право добрать баллы во время консультаций, назначенных преподавателем.

6. Преподаватель несет ответственность за правильность подсчета итоговых баллов.

7. Преподаватель не имеет права аннулировать баллы, полученные студентом во время семестра, обязан учитывать их при выведении итоговой оценки.

Распределение рейтинговых баллов по дисциплине

По дисциплине «Защита информации» предусмотрено два дисциплинарных модуля.

1 семестр

Дисциплинарный модуль	ДМ 1.1	ДМ 1.2
Текущий контроль (лабораторные работы)	9-16	12-20
Текущий контроль (контрольная работа)	-	-
Текущий контроль (тестирование)	8 - 14	6-10
Общее количество баллов	17-30	18-30
Итоговый балл:	35-60	

Дисциплинарный модуль 1.1

№ п/п	Виды работ	Максимальный балл
Текущий контроль		
1	Лабораторное занятие 1-2. Алгоритм RSA	5
2	Лабораторное занятие 3-4. Алгоритм DSA	5
3	Лабораторное занятие 5-6. Схема Эль-Гамала.	6
Итого:		16
Текущий контроль		
1	Тестирование по модулю 1.1	14
Итого:		30

Дисциплинарный модуль 1.2

№ п/п	Виды работ	Максимальный балл
Текущий контроль		
1	Лабораторное занятие 7-8. Простая и двойная перестановки.	3
2	Лабораторное занятие 9-10. Одиночная перестановка по ключу.	3
3	Лабораторное занятие 11-12. Шифр Цезаря.	3
4	Лабораторное занятие 13-14. Шифр Виженера. Шифр Вернама.	3
5	Лабораторное занятие 15-16. Хэш-функция MD5.	4
6	Лабораторное занятие 17-18. Хэш-функция SHA.	4
Итого:		20
Текущий контроль		
1	Тестирование по ДМ 1.2	10
Итого:		30

2 семестр

Распределение рейтинговых баллов по дисциплинарным модулям

Дисциплинарный модуль	ДМ 2.1	ДМ 2.2
Текущий контроль (лабораторные работы)	10-20	11-20
Текущий контроль (контрольная работа)	-	-
Текущий контроль (тестирование)	7-10	7-10
Общее количество баллов	17-30	18-30
Итоговый балл:	35-60	

Дисциплинарный модуль 2.1.

№ п/п	Виды работ	Максимальный балл
Текущий контроль		
1	Лабораторное занятие 19. Линейный конгруэнтный метод генерации псевдослучайных чисел	6
2	Лабораторное занятие 20-21. Алгоритм Блюма-Блюма-Шума.	6
3	Лабораторное занятие 22-23. Алгоритм xor-shift.	8
Итого:		20
Текущий контроль		
1	Тестирование по модулю 2.1	10
Итого:		30

Дисциплинарный модуль 2.2.

№ п/п	Виды работ	Максимальный балл
Текущий контроль		
1	Лабораторное занятие 24. Стандарт цифровой подписи DSS. Генерация цифровой подписи.	4
2	Лабораторное занятие 25-26. Изучение американского стандарта шифрования данных DES.	8
3	Лабораторное занятие 27. Изучение отечественного стандарта шифрования данных ГОСТ 28147-89.	8
Итого:		20
Текущий контроль		
1	Тестирование по модулю 2.2.	10
Итого:		30

Студентам могут быть добавлены **дополнительные баллы** за следующие виды деятельности:

- участие в научно-исследовательской работе кафедры (до 7 баллов);
- выступление с докладами (по профилю дисциплины) на конференциях различного уровня (до 5 баллов);
- участие в написании статей с преподавателями кафедры (до 5 баллов);
- участие в тематических Круглых столах, проводимых кафедрой математики и информатики (до 5 баллов), на олимпиадах в других вузах (до 10 баллов).

При этом, если в течение семестра студент набирает более 60 баллов (по результатам дисциплинарных модулей и полученных дополнительных баллов), то итоговая сумма баллов округляется до 60 баллов.

В соответствии с Учебным планом направления подготовки 38.03.01 - «Экономика» по дисциплине «Защита информации» предусмотрен **экзамен и зачет**.

Критерии оценки знаний студентов в рамках итогового контроля в форме экзамена

-устно

№ п/п	Структура экзаменационного билета	Максимальный балл
1	Теоретическая часть	40
Итого за экзамен		40

Для получения экзаменационной оценки общая сумма баллов (за дисциплинарные модули и экзамен) должна составлять от 55 до 100 баллов (см. шкалу перевода рейтинговых баллов).

- в форме компьютерного тестирования

На экзамене, который проводится в форме компьютерного тестирования, студенту предоставляется блок тестовых заданий в количестве 40 шт., которые генерируются автоматической тестирующей системой персонально в случайном порядке и содержат вопросы по всему перечню тем дисциплины. Каждое правильно выполненное тестовое задание оценивается в 1 балл. Максимальное количество баллов, которое студент имеет возможность набрать – 40.

Для получения экзаменационной оценки общая сумма баллов (за дисциплинарные модули и экзамен) должна составлять от 55 до 100 баллов (см. шкалу перевода рейтинговых баллов).

На промежуточной аттестации подводятся итоги сформированности компетенций в виде комплексной оценки знаний, умений, владений по компетенции: ОПК-1, ПК-10.

Шкала перевода рейтинговых баллов

Общее количество набранных баллов	Оценка
55-70	3 (удовлетворительно)
71-85	4 (хорошо)
86-100	5 (отлично)

7. Перечень основной, дополнительной учебной литературы и учебно-методических изданий, необходимых для освоения дисциплины

№ п/п	Библиографическое описание	Количество печатных экземпляров или адрес электронного ресурса	Коэффициент обеспеченности
Основная литература			
1.	Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных [Электронный ресурс]: учебное пособие / С. Н. Никифоров, М. М. Ромаданов. —	Режим доступа: http://www.iprbookshop.ru/80747.html	1

	Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 108 с.		
2.	Бутакова, Н. Г. Криптографические методы и средства защиты информации [Электронный ресурс]: учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2017. — 384 с.	Режим доступа: http://www.iprbookshop.ru/66791.html	1
3.	Алексеев, А. П. [Электронный ресурс]: Многоуровневая защита информации / А. П. Алексеев. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017. — 128 с.	Режим доступа: http://www.iprbookshop.ru/75387.html	1
Дополнительная литература			
1.	Краковский, Ю. М. Защита информации [Электронный ресурс]: учебное пособие / Ю. М. Краковский. — Ростов-на-Дону : Феникс, 2016. — 349 с.	Режим доступа: http://www.iprbookshop.ru/59350.html	1
2.	Соколов, В. П. Кодирование в системах защиты информации [Электронный ресурс] : учебное пособие / В. П. Соколов, Н. П. Тарасова ; под редакцией О. И. Шелухин. — Москва : Московский технический университет связи и информатики, 2016. — 94 с.	Режим доступа: http://www.iprbookshop.ru/61485.html	1
3.	Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом [Электронный ресурс]: учебное пособие / Ю. А. Котов. — Новосибирск : Новосибирский государственный технический университет, 2017. — 67 с.	Режим доступа: http://www.iprbookshop.ru/91227.html	1
Учебно-методические издания			
1.	Потапова О.Н. Защита информации: методические указания по выполнению лабораторных работ и организации самостоятельной работы по дисциплине «Защита информации» для бакалавров направления подготовки 38.03.01 «Экономика»	http://elibrary.agni-rt.ru	1

	всех форм обучения. - Альметьевск: тип. АГНИ, 2016.		
--	--	--	--

8. Перечень профессиональных баз данных, информационных справочных систем и информационных ресурсов, необходимых для освоения дисциплины

№ п/п	Наименование	Адрес в Интернете
1	Единое окно доступа к информационным ресурсам	http://window.edu.ru/
2	Российская государственная библиотека	http://www.rsl.ru
3	Электронная библиотека Elibrary	http://elibrary.ru
4	Электронно-библиотечная система IPRbooks	http://iprbookshop.ru
5	Электронная библиотека АГНИ	http://elibrary.agni-rt.ru

9. Методические указания для обучающихся по освоению дисциплины

Цель методических указаний по освоению дисциплины – обеспечить обучающемуся оптимальную организацию процесса изучения дисциплины, а также выполнения различных форм самостоятельной работы.

Изучение дисциплины обучающимся требует систематического, упорного и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить как пропущенную тему, так и всю дисциплину в целом. Именно поэтому контроль над систематической работой студентов должен находиться в центре внимания преподавателя.

При подготовке к лекционным занятиям (теоретический курс) обучающимся необходимо:

- перед очередной лекцией необходимо изучить по конспекту материал предыдущей лекции, просмотреть рекомендуемую литературу;
- при затруднениях в восприятии материала следует обратиться к основным литературным источникам, рекомендованным рабочей программой дисциплины. Если разобраться в материале самостоятельно не удалось, то следует обратиться к лектору (по графику его консультаций) или к преподавателю на практических, лабораторных занятиях.

При подготовке к лабораторным работам, обучающимся необходимо:

- приносить с собой рекомендованную в рабочей программе литературу к конкретному занятию;
- до очередного лабораторного занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей теме;
- теоретический материал следует соотносить с нормативно-справочной литературой, так как в ней могут быть внесены последние научные и практические достижения, изменения, дополнения, которые не всегда отражены в учебной литературе;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов, в случае затруднений – обращаться к преподавателю.

Обучающимся, пропустившим занятия (независимо от причин), рекомендуется не позже, чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии.

Самостоятельная работа студентов имеет систематический характер и складывается из следующих видов деятельности:

подготовка ко всем видам контрольных испытаний, в том числе к текущему контролю успеваемости (в течение семестра), промежуточной аттестации (по окончании семестра),

- самостоятельное изучение теоретического материала;
- подготовка к выполнению лабораторных работ.

Для выполнения указанных видов работ необходимо изучить соответствующие темы теоретического материала, используя конспект лекций, учебники и учебно-методическую литературу, а также интернет-ресурсы.

Перечень учебно-методических изданий, рекомендуемых студентам для подготовки к занятиям и выполнению самостоятельной работы, а также методические материалы на бумажных и/или электронных носителях, выпущенные кафедрой своими силами и предоставляемые студентам во время занятий, представлены в пункте 7 рабочей программы.

Учебно-методическая литература для данной дисциплины имеется в электронно-библиотечной системе «IPRbooks», доступ к которым предоставлен студентам, а также на электронном ресурсе АГНИ (<http://elibrary.agni-rt.ru>), доступ к которым предоставлен студентам.

10. Перечень информационных технологий

№ п/п	Наименование программного обеспечения	Лицензия	Договор
1	Microsoft Office Professional Plus 2016 Rus Academic OLP (Word, Excel, PowerPoint, Access)	№67892163 от 26.12.2016г.	№ 0297/136 от 23.12.2016г.
2	Microsoft Office Standard 2016 Rus Academic OLP (Word, Excel, PowerPoint)	№67892163 от 26.12.2016г.	№ 0297/136 от 23.12.2016г.
3	Microsoft Windows Professional 10 Rus Upgrade Academic OLP	№67892163 от 26.12.2016г.	№ 0297/136 от 23.12.2016г.
4	ABBYY Fine Reader 12 Professional	№197059 от 26.12.2016г.	№ 0297/136 от 23.12.2016г.
5	Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition	№ 24С41712081012212531 138	№ 791 от 30.11.2017г.
6	Электронно-библиотечная система IPRbooks		Государственный контракт №595 от 30.10.2017г.
7	ПО «Автоматизированная тестирующая система»	Свидетельство государственной регистрации программ для ЭВМ №2014614238	

		от 01.04.2014г.	
8	7-Zip File Manager	Свободно распространяемое ПО	

11. Материально-техническая база, необходимая для осуществления образовательного процесса по данной дисциплине

Освоение дисциплины «Защита информации» предполагает использование нижеперечисленного материально-технического обеспечения:

№ п/п	Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Ул. Р. Фахретдина, 42. Учебный корпус В, аудитория В-134 учебная аудитория для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	1. Компьютер в комплекте с монитором 2. Проектор BenQ MX704 3. Экран с электроприводом
2.	Ул. Р. Фахретдина, 42. Учебный корпус В, аудитория В-308 компьютерный класс (учебная аудитория для проведения занятий практического и лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы)	1. Компьютер в комплекте с монитором IT Corp 3250 – 11 шт. с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду института. 2. Проектор BenQ MX717 3. Экран на штативе 4. Принтер HP LJ P3015d 5. Сканер Epson Perfection V33
3.	Ул. Р. Фахретдина, 42. Учебный корпус В, аудитория В-319 компьютерный класс (учебная аудитория для проведения занятий практического и лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы)	1. Компьютер в комплекте с монитором IT Corp 3260 – 11 шт. с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду института. 2. Проектор BenQ MX717 3. Экран на штативе 4. Принтер Kyocera FS-2100dn 5. Сканер Epson Perfection V33
4.	Ул. Р. Фахретдина, 42. Учебный корпус В, аудитория В-408 компьютерный класс (учебная аудитория для проведения занятий практического и лабораторного типа, групповых	1. Компьютер в комплекте с монитором IT Corp 3250 – 14 шт. с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду института. 2. Проектор BenQ MX704 3. Экран на штативе

	и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы)	4. Принтер HP LJ P3015d 5. Сканер Epson Perfection V33
5.	Ул. Ленина, 2. Учебный корпус А, аудитория А-326 компьютерный класс (учебная аудитория для проведения занятий практического и лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы)	1. Компьютер в комплекте с монитором IT Corp H110 – 10 шт. с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду института. 2. Принтер HP LJ P2015d 3. Сканер Epson Perfection V33
6.	Ул. Ленина, 2. Учебный корпус А, аудитория А-318 учебная аудитория для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	1. Компьютер в комплекте с монитором с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду института. 2. Проектор BenQ MX704 3. Экран с электроприводом

*Специальные помещения – учебные аудитории для проведения занятий лекционного типа, практических и лабораторных занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися лицам с ограниченными возможностями здоровья:

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем;

- применение дистанционных образовательных технологий для организации форм текущего контроля;

- увеличение продолжительности сдачи обучающимся лицам с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут.

Рабочая программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению подготовки 38.03.01 – «Экономика» направленности (профиля) подготовки «Экономика предприятий и организаций».

**АННОТАЦИЯ
рабочей программы дисциплины**

«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки
38.03.01 – Экономика

Направленность (профиль) подготовки
«Экономика предприятий и организаций»

Оцениваемые компетенции (код, наименование)	Результаты освоения компетенции	Оценочные средства текущего контроля и промежуточной аттестации
<p>ОПК-1 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p>Знать: -основы системы информационной и библиографической культуры; -основы информационно-коммуникационных технологий; -основные требования информационной безопасности при решении задач профессиональной деятельности. Уметь: -анализировать библиографический и информационный материал используя информационно -коммуникационные технологии; -определять стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности. Владеть: -навыками анализа профессионально-практической деятельности работы с использованием основных требований информационной безопасности с применением информационно-коммуникационных технологий.</p>	<p>Текущий контроль: Компьютерное тестирование по темам 1- 9 Лабораторные работы по темам 3-6, 8, 9</p> <p>Промежуточная аттестация: 1 семестр Зачет 2 семестр Экзамен</p>
<p>ПК-10 Способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии</p>	<p>Знать: - основные методы решения коммуникативных задач; - специфику различных способов решения коммуникативных задач; - современные технические средства и информационные технологии, используемые при</p>	<p>Текущий контроль: Компьютерное тестирование по темам 1- 9 Лабораторные работы по темам 3-6, 8, 9</p> <p>Промежуточная аттестация:</p>

	<p>решении коммуникативных задач;</p> <p>Уметь:</p> <p>- пользоваться современными техническими средствами и информационными технологиями при решении коммуникативных задач.</p> <p>Владеть:</p> <p>- навыками для самостоятельного, методически правильного решения коммуникативных задач;</p> <p>- техническими средствами и информационными технологиями при решении коммуникативных задач.</p>	<p>1 семестр Зачет</p> <p>2 семестр Экзамен</p>
--	--	---

Место дисциплины в структуре ОПОП ВО	Б1.В.ДВ.06.02 Дисциплина «Защита информации» является дисциплиной по выбору, входит в состав Блока 1 «Дисциплины (модули)» и относится к вариативной части ОПОП. Осваивается на 1 курсе в 1 и 2 семестрах ¹ / на 1 курсе в 1 семестре ²	
Общая трудоемкость дисциплины (в зачетных единицах и часах)	Зачетных единиц по учебному плану: 6 ЗЕ . Часов по учебному плану: 216 ч .	
Виды учебной работы	Контактная работа обучающихся с преподавателем 94ч ¹ /22 ч ² : - лекции 36 ¹ /8 ч. ² ; - лабораторные работы 54 ¹ /8 ч. ² .; - КСР 4 ¹ /6 ч. ² . Самостоятельная работа 86 ¹ /185 ч. ² .	
Изучаемые темы (разделы)	<p>Тема 1. Основные понятия и определения в области информационной безопасности. Концептуальная модель информационной безопасности</p> <p>Тема 2. Исследование причин нарушений безопасности.</p> <p>Тема 3. Ассиметричные системы шифрования.</p> <p>Тема 4. Традиционное шифрование: классические методы. Криптостойкость.</p> <p>Тема 5. Хэш-функции и аутентификация сообщений.</p> <p>Тема 6. Алгоритмы генерации псевдослучайных последовательностей чисел.</p> <p>Тема 7. Архитектура защищенных операционных систем.</p> <p>Тема 8. Электронная цифровая подпись.</p> <p>Тема 9. Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.</p>	
Форма промежуточной аттестации	Зачет в 1 семестре, экзамен во 2 семестре ¹ / зачет и экзамен на 1 курсе ²	

¹ Очная форма обучения

² Заочная форма обучения

