МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

_____ Ю.В. Добржинский
01 сентября 2017г.

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Ю.В. Добржинской
01 сентября 2017г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Защита информации
Направление подготовки 09.03.01 Информатика и вычислительная техника

Форма подготовки очная

курс 4 семестр 7
лекции 36 час.
практические занятия _____час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 22 / пр. _____/ лаб. _____час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 22 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену_____час.
контрольные работы (количество)_____
курсовая работа / курсовой проект _____семестр
зачет 7 Семестр
экзамен _____семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно установленного ДВФУ по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденный приказом ректора ДВФУ от 04.04.2016 № 12-13-593.

Рабочая программа обсуждена на заседании кафедры «Информационная безопасность», протокол № 13 от 30 июня 2017г.

И.о. заведующего кафедрой «Информационная безопасность» Добржинский Ю.В., к.т.н., с.н.с.
Составитель: Чусов А.А.

I. Рабочая программа пересмотрена на заседании кафедры:
Протокол от«_____»_____20 г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:
Протокол от«_____»_____20 г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Bachelor's degree in Computer science and computer facilities (09.03.01)

Study profile "Computer Systems and Networks"

Course title: Data protection

Variable part of Block, 4 credits

Instructor: Chusov A.A.

At the beginning of the course a student should be able to:

- self-improvement and self-development in the professional sphere, to increase the general cultural level (GC-1);
- self-organization and self-education (GC-14);
- master the methods of using software to solve practical problems (GPC-2);
- participate in setup and adjustment of hardware and software systems (GPC-4).

Learning outcomes:

- the ability to solve standard problems of professional activity on the basis of information and bibliographic culture with the use of information and communication technologies and taking into account the basic information security requirements (GPC-5);
- the ability to develop and maintain requirements for individual functions of the system (SPC-2).

Course description: this course includes the following main sections: the main directions of information protection, organizational and administrative methods of information protection, software and hardware protection of computer systems.

Main course literature:

1. Zhuk AP, Zhuk EP, Lepeshkin OM, Timoshkin A.I. Protection of Information: Tutorial / A.P. Zhuk, E.P. Zhuk, OM Lepeshkin, A.I. Timoshkin - M.: RIOR, 2015. - 392 p. - Access mode: http://znanium.com/catalog/product/474838

2. Karatunova N.G. Protection of information. Course / N.G. Karatunova - Krasnodar: KSEI, 2014. - 188 p. - Access mode: http://znanium.com/catalog/product/503511

3. Malyuk A.A. Protection of information in the information society / A.A. Malyuk - M.: Gore. Line-Telecom, 2015. - 230 p. - Access mode: http://znanium.com/catalog/product/536930

Form of final knowledge control: *pass-fail exam.*

Аннотация к рабочей программе дисциплины
«Защита информации»

Рабочая программа дисциплины «Защита информации» разработана для студентов 4 курса специальности 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления».

Трудоемкость дисциплины в зачетных единицах составляет 4 з.е., в академических часах – 144 часа (лекции – 36 часов, лабораторная работа – 36 часов, самостоятельная работа – 72 часа). Дисциплина реализуется на 4 курсе в 7 семестре.

Дисциплина «Защита информации» является вариативной частью с кодом Б1.В.ДВ.6.1 и базируется на предварительном изучении следующих дисциплин: «Математическая логика и теория алгоритмов», «Основы дискретной математики», «Введение в программирование», «Основы и методы программирования», что обеспечивает лучшее усвоение материала и дает целостную картину о современном состоянии и развитии систем защиты информации.

Данная дисциплина включает такие вопросы, как основные направления защиты информации, организационные и административные методы защиты информации, программно-аппаратные средства защиты компьютерных систем. Теоретический материал курса подкрепляется лабораторными заданиями в программе для шифрования информации GnuPG.

Цель дисциплины – изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи дисциплины:

- сформировать у студентов представления об основных типах и способах защиты информации;
- развить навыки проектирования системы защиты информации;
- развить навыки владения современными программными и аппаратными средствами защиты информации
- воспитать профессионально значимые личностные качества;
- сформировать представление о важности учебной дисциплины для осуществления будущей профессиональной деятельности.

Для успешного изучения дисциплины «Защита информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность к самосовершенствованию и саморазвитию в

профессиональной сфере, к повышению общекультурного уровня (ОК-1);

- способность к самоорганизации и самообразованию (ОК-14);
- способность осваивать методики использования программных средств для решения практических задач (ОПК-2);
- способность участвовать в настройке и наладке программно-аппаратных комплексов (ОПК-4).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-5) способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знает	Принципы обеспечения информационной безопасности; основы информационной безопасности и защиты информации; типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; типовые разработанные средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных систем.
	Умеет	Определять основные угрозы информационной безопасности на предприятии (в организации); осуществлять обоснованный выбор средств и систем защиты информации; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации.
	Владеет	Методиками анализа предметной области; навыками применения технических средств защиты информации; навыками администрирования систем и устройств защиты информации.
(ПК-2) способность разрабатывать и сопровождать требования к отдельным функциям системы	Знает	Основные понятия и направления в защите компьютерной информации; принципы защиты информации; принципы классификации и примеры угроз безопасности компьютерным системам; современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности.

	Умеет	Конфигурировать встроенные средства безопасности в операционной системе; устанавливать и использовать один из межсетевых экранов; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настроить инструменты резервного копирования и восстановления информации.
	Владеет	Методами аудита безопасности информационных систем; методами системного анализа информационных систем.

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита информации» применяются следующие методы активного/ интерактивного обучения: проблемная лекция, чтение лекций с использованием мультимедийного оборудования, выполнение лабораторных работ в программе для шифрования информации GnuPG.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Введение в информационную безопасность (8 час.)

Тема 1. Основные определения и понятия в защите информации (8 час.)

1.1 Основные определения: информационная безопасность, защищенная система, защита информации.

1.2 Концептуальные основы информационной безопасности и защиты информации.

Раздел II. Защита информации (28 час.)

Тема 1. Организационно-правовые аспекты защиты информации (8 час.)

1.1 Современное состояние проблемы информационной безопасности.

1.2 Организационно-правовые методы информационной безопасности.

Тема 2. Политика безопасности и управление рисками. (8 час.)

2.1 Угрозы информационной безопасности.

2.2 Роль стандартов в обеспечении информационной безопасности.

Тема 3. Программно-технические методы защиты информации (6 час.)

3.1 Системы обеспечения комплексной безопасности информации.

3.2 Безопасность компьютерных сетей.

Тема 4. Криптографические методы защиты информации (6 час.)

4.1 Введение в криптографические методы защиты.

4.2 Криптографические методы защиты информации.

II. СТРУКТУРА И СОДЕРЖАНИЕ ЛАБОРАТОРНОЙ И ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (36 час.)

Лабораторная работа №1. Основы шифрования данных (16 час.)

1. Изучение основных принципов шифрования информации.
2. Знакомство с широко известными алгоритмами шифрования.
3. Приобретение навыков программной реализации алгоритмов шифрования.

Лабораторная работа №2. Ассиметричная криптография (20 час.)

4. Знакомство с принципами криптографической защиты информации с использованием алгоритмов асимметричного шифрования.
5. Приобретение навыков практического применения методов защиты информации на основе системы GnuPG.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Защита информации» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы;
- критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№	Контролируемые	Коды и этапы	Оценочные средства -

п/п	разделы / темы дисциплины	формирования компетенций		наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в информационную безопасность	ПК-2	знает	ПР-7	УО-1
			умеет	ПР-6	УО-1
			владеет	ПР-6	УО-1
2	Раздел II. Защита информации	ОПК-5, ПК-2	знает	ПР-7	УО-1
			умеет	ПР-6	УО-1
			владеет	ПР-6	УО-1

Фонд оценочных средств, определяющий процедуру оценивания знаний, умений и навыков и (или) опыта деятельности; критерии и показатели, необходимые для оценки знаний, умений, навыков, а также оценочные средства для промежуточной аттестации и список вопросов на зачет представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература
(электронные и печатные издания)

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин – М. : РИОР, 2015. — 392 с. — Режим доступа: http://znanium.com/catalog/product/474838

2. Каратунова Н.Г. Защита информации. Курс / Н.Г. Каратунова — Краснодар : КСЭИ, 2014. — 188 с. — Режим доступа: http://znanium.com/catalog/product/503511

3. Малюк А.А. Защита информации в информационном обществе / А.А. Малюк — М. : Гор. линия-Телеком, 2015. — 230 с. — Режим доступа: http://znanium.com/catalog/product/536930

Дополнительная литература
(печатные и электронные издания)

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по

техническим каналам / Г.А. Бузов — М. : Гор. линия-Телеком, 2015. — 586 с. — Режим доступа: http://znanium.com/catalog/product/895240

2. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность и защита информации / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова — М. : РИОР, 2013. — 222 с. — Режим доступа: http://znanium.com/catalog/product/405000

3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах / В.Ф. Шаньгин — М. : ФОРУМ, 2013. — 592 с. — Режим доступа: http://znanium.com/catalog/product/402686

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Список лекций по основам информатики и вычислительной техники [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1
2. Способы защиты информации [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/
3. Криптографические методы защиты информации [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://sec4all.net/modules/myarticles/article.php?storyid=605

Перечень информационных технологий и программного обеспечения

Для выполнения лабораторного задания используется программа для шифрования информации GnuPG 1.4.7. Для работы с литературой из списка необходимо наличие у студента аккаунтов в указанных электронно-библиотечной системе: «Znanium.com» (http://znanium.com/) .

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита информации», составляет 72 часа. На самостоятельную работу – 72 часа.

Аудиторная нагрузка состоит из 36 лекционных часов и 36 часов лабораторных работ. На лекционных занятиях обучающийся получает теоретические знания, усвоение которых необходимо для дальнейшего выполнения лабораторных работ. Студенту рекомендуется предварительно

готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

Подготовка к лабораторным работам предполагает повторение лекционного материала. В результате выполнения работы студент предоставляет преподавателю отчёт о проделанной работе, содержащий следующие пункты: цель работы, краткий теоретический материал, задание, ход работы, результаты и выводы о проделанной работе.

В рамках указанной дисциплины итоговой формой аттестации является зачет. Вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях. Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников из списка литературы и материалов по лабораторным работам.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения лекционных занятий и лабораторных работ необходима оборудованная персональными компьютерами аудитория с мультимедиа проектором.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Защита информации»

Направление подготовки 09.03.01 Информатика и вычислительная техника

профиль «Автоматизированные системы обработки информации и управления»

Форма подготовки очная

Владивосток
2016

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-9 неделя обучения	Подготовка лабораторной работы (выполнение отчета к лабораторной работе №1)	32	Отчет о выполнении
2	10-17 неделя обучения	Подготовка лабораторной работы (выполнение отчета к лабораторной работе №2)	31	Отчет о выполнении
3	18 неделя обучения	Подготовка к зачету	9	Зачет

Подготовка отчета по лабораторным работам предполагает повторение лекционного материала и выполнение задания для лабораторных работ по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовить для сдачи отчёт по проделанной работе. Необходимо указать в отчёте следующую информацию: название и цель работы, краткий теоретический материал, задание на лабораторную работу, ход работы, полученные результаты и выводы. По результатам защиты отчёта студенту выставляется «зачтено» или «не зачтено». Студент получает «зачтено», если отчёт содержит все перечисленные ранее пункты и оформлен в соответствии с правилами оформления письменных работ.

Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к зачету, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД.

Приложение 2

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Защита информации»
Направление подготовки 09.03.01 Информатика и вычислительная техника
профиль «Автоматизированные системы обработки информации и управления»
Форма подготовки очная

Владивосток
2016

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-5) способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знает	Принципы обеспечения информационной безопасности; основы информационной безопасности и защиты информации; типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; типовые разработанные средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных систем.
	Умеет	Определять основные угрозы информационной безопасности на предприятии (в организации); осуществлять обоснованный выбор средств и систем защиты информации; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации.
	Владеет	Методиками анализа предметной области; навыками применения технических средств защиты информации; навыками администрирования систем и устройств защиты информации.
(ПК-2) способность разрабатывать и сопровождать требования к отдельным функциям системы	Знает	Основные понятия и направления в защите компьютерной информации; принципы защиты информации; принципы классификации и примеры угроз безопасности компьютерным системам; современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности.
	Умеет	Конфигурировать встроенные средства безопасности в операционной системе; устанавливать и использовать один из межсетевых экранов; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настроить инструменты резервного копирования и восстановления информации.
	Владеет	Методами аудита безопасности информационных систем; методами системного анализа информационных систем.

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в информационную безопасность	ПК-2	знает	ПР-7	УО-1
			умеет	ПР-6	УО-1
			владеет	ПР-6	УО-1
2	Раздел II. Защита информации	ОПК-5, ПК-2	знает	ПР-7	У-О-1
			умеет	ПР-6	УО-1
			владеет	ПР-6	УО-1

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ОПК-5) способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	знает (порого-вый уровень)	Принципы обеспечения информационной безопасности; основы информационной безопасности и защиты информации; типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; типовые разработанные средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.

информационной безопасности		систем.		
	умеет (продвинутый)	Определять основные угрозы информационной безопасности на предприятии (в организации); осуществлять обоснованный выбор средств и систем защиты информации; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно определять основные угрозы информационной безопасности, осуществлять обоснованный выбор средств и систем защиты информации самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	владеет (высокий)	Методиками анализа предметной области; навыками применения технических средств защиты информации; навыками администрирования систем и устройств защиты информации.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно применить технические средства защиты информации, администрировать системы и устройства защиты информации .
(ПК-2) способность разрабатывать и сопровождать требования к отдельным функциям системы	знает (пороговый уровень)	Основные понятия и направления в защите компьютерной информации; принципы защиты информации; принципы классификации и примеры угроз безопасности компьютерным системам; современные подходы к защите продуктов и систем	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.

		информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности.		
	умеет (продвинутый)	Конфигурировать встроенные средства безопасности в операционной системе; устанавливать и использовать один из межсетевых экранов; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настроить инструменты резервного копирования и восстановления информации.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно устанавливать и использовать один из межсетевых экранов и настраивать программное обеспечение для защиты от вредоносного программного обеспечения самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	владеет (высокий)	Методами аудита безопасности информационных систем; методами системного анализа информационных систем.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно провести аудит безопасности и системный анализ информационных систем.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачет.

Для допуска к зачету обучающийся должен получить оценку «зачтено» по всем лабораторным работам курса. Критерии оценивания лабораторных работ представлены далее в данном Приложении.

Зачет проводится в форме собеседования (УО-1), вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. Для подготовки к ответу на зачете обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки учитываются:

- знание основных терминов и понятий курса;
- знание и владение методами и средствами решения задач;
- последовательное изложение материала курса;
- умение формулировать некоторые обобщения по теме вопросов;
- достаточно полные ответы на вопросы;
- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для промежуточной аттестации
Список вопросов на зачет

1. Информационная безопасность. Основные определения.
2. Концептуальные основы информационной безопасности и защиты информации.
3. Современное состояние проблемы информационной безопасности.
4. Организационно-правовые методы информационной безопасности.
5. Угрозы информационной безопасности.
6. Стандарты информационной безопасности.
7. Системы обеспечения комплексной безопасности информации.
8. Безопасность компьютерных сетей.
9. Примеры платных и бесплатных антивирусных программ. Выделить достоинства и недостатки.
10. Идентификация, аутентификация и авторизация.
11. Функции межсетевых экранов.
12. Проблемы обеспечения безопасности операционных систем.
13. Основы работы антивирусных программ.
14. Особенности функционирования межсетевых экранов.
15. Системы шифрования данных. Примеры систем.
16. Асимметричные криптосистемы шифрования.

Каждый студент должен ответить на два вопроса из списка выше. Результаты зачета оцениваются по двухбалльной системе («зачтено», «не зачтено») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

- знание основных терминов и понятий курса;
- знание и владение методами и средствами решения задач;
- последовательное изложение материала курса;
- умение формулировать некоторые обобщения по теме вопросов;
- достаточно полные ответы на вопросы;
- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«зачтено».** Хорошее знание основных терминов и понятий курса. Хорошее знание и владение методами и средствами решения задач. Последовательное изложение материала курса. Умение формулировать некоторые обобщения по теме вопросов. Достаточно полные ответы на вопросы. Умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«не зачтено».** Неудовлетворительное знание основных терминов и понятий курса. Неумение решать задачи. Отсутствие логики и последовательности в изложении материала курса. Немение формулировать отдельные выводы и обобщения по теме вопросов. Неумение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются лабораторные работы (ПР-6) и конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников

	литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.

Оценка продвинутого и высокого уровня сформированности компетенции проводятся на основе результатов выполнения лабораторных работ. Темы лабораторных работ представлены в Разделе II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	**Критерий**
Зачтено	Отчёт по лабораторной работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на лабораторную работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ.
Незачтено	Отчёт по лабораторной работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ.