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. Добржинский
01 сентября 2017г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Безопасность вычислительных систем
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._____/ пр. _____/ лаб. _____час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО _____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: старший преподаватель Смирнов М.Е.

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: *Security of computing systems*

Variable part of Block, 4 credits

Instructor:

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);*
- *develop business plans and technical assignments for equipping departments, laboratories, offices with computer and network equipment (GPC-3);*
- *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 the protection of the computer system, methods of protecting the information of the computing system, software and hardware means of protecting computing systems.*

Main course literature:

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. — М. : Форум, 2013. — 368 с.

2. Дубинин Е.А., Тебуева Ф.Б., Копытов В.В. Оценка относительного ущерба безопасности информационной системы / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. — М. : РИОР, 2014. — 192 с.

3. Девянин П.Н. Модели безопасности компьютерных систем / П.Н. Девянин — М. : Гор. линия-Телеком, 2012. — 320 с.

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

АННОТАЦИЯ

Рабочая программа дисциплины «Безопасность вычислительных систем» разработана для студентов 4 курса специальности 09.03.01 «Информатика и вычислительная техника», профиль «Вычислительные машины, комплексы, системы и сети».

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 «Безопасность вычислительных систем» является вариативной частью с кодом Б1.В.ДВ.6.2 и базируется на предварительном изучении следующих дисциплин: «Основы вычислительной техники», «История информационных систем управления», «Введение в программирование», «Основы и методы программирования», что обеспечивает лучшее усвоение материала и дает целостную картину о современном состоянии и развитии безопасности вычислительных систем.

Данная дисциплина включает такие вопросы, как основные направления защиты вычислительной системы, методы защиты информации вычислительной системы, программно-аппаратные средства защиты вычислительных систем. Теоретический материал курса подкрепляется лабораторными заданиями в текстовом редакторе Microsoft Word 2010.

Цель дисциплины – заложить практические правила управления безопасностью вычислительных систем, научить комплексному подходу к обеспечению безопасности, научить проводить анализ угроз безопасности, приобрести навыки анализа рисков безопасности; изучить методы и средства обеспечения безопасности вычислительных систем.

Задачи дисциплины:

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

Для успешного изучения дисциплины «Безопасность вычислительных систем» 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 разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием (ОПК-3);
- 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	Порядок и методику проведения оценки информационной безопасности; как получать свидетельства оценки и на основе их устанавливать степени выполнения заданных требований по обеспечению информационной безопасности.
	Умеет	Определять основные угрозы информационной безопасности вычислительной системы; осуществлять обоснованный выбор средств и систем защиты информации; реализовывать мероприятия для обеспечения деятельности в области защиты информации.
	Владеет	Навыком формирования требований к средствам защиты информации.
(ПК-2) способность разрабатывать и сопровождать требования к отдельным функциям системы	Знает	Основные требования нормативно-правовой базы информационной безопасности к защите корпоративных информационных систем и их компонентов от несанкционированного доступа к информации, программных средств скрытого информационного воздействия, утечки информации по техническим каналам.
	Умеет	Применять методы определения причин, видов, источников и каналов утечки, искажения информации.

	Владеет	Анализом оценки информационной безопасности и имеет навык устанавливать степени выполнения заданных требований по обеспечению безопасности вычислительной системы.

Для формирования вышеуказанных компетенций в рамках дисциплины «Безопасность вычислительных систем» применяются следующие методы активного/интерактивного обучения: чтение лекций, чтение лекций с использованием мультимедийного оборудования (проектор), выполнение лабораторных работ в текстовом редакторе Microsoft Word 2010.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Введение в безопасность вычислительных систем (8 час.)

Тема 1. Основные понятия и определения (8 час.)

1.1 Основные определения: информационные системы, вычислительные системы.

1.2 Безопасность корпоративных информационных систем.

Раздел II. Безопасность вычислительных систем (28 час.)

Тема 1. Организационно-методологические основы оценки информационной безопасности (6 час.)

1.1 Методологии безопасности.

1.2 Организационно-методологические основы построения защищенных вычислительных систем.

Тема 2. Каналы утечки информации в вычислительной системе. (6 час.)

2.1 Модель нарушителя. Классы нарушителей.

2.2 Перечень каналов утечки информации.

2.3 Описание вредоносных воздействий на данные.

Тема 3. Методы и средства защиты информации (8 час.)

3.1 Классификация методов и средств защиты информации.

3.2 Инвентаризация методов и средств защиты информации.

3.3 Анализ степени перекрытия каналов утечки информации.

Тема 4. Анализ защищенности данных вычислительных систем. (8 час.)

4.1 Оценка выполнения требований по обеспечению защиты от несанкционированного доступа к информации в корпоративных информационных системах.

4.2 Оценка выполнения требований к процессам системы управления информационной безопасностью.

4.3 Оценка выполнения требований к организационно-правовому обеспечению применения средств защиты информации.

4.4 Оценка выполнения требований по обеспечению защиты информации от вредоносных программ.

II. СТРУКТУРА И СОДЕРЖАНИЕ ЛАБОРАТОРНОЙ И ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (36 час.)

Лабораторная работа №1. Нормативно-правовая база информационной безопасности вычислительных систем (12 час.)

1. Знакомство со стандартами и нормативно-методическими документами в области обеспечения информационной безопасности.
2. Изучение государственной системы обеспечения информационной безопасности и международных правовых актов по защите информации.
3. Приобретение навыков создания, утверждения и исполнения инструкций (в том числе должностных).

Лабораторная работа №2. Анализ защищенности данных вычислительных систем (24 час.)

4. Приобретение навыка оценки выполнения требований по обеспечению защиты от несанкционированного доступа к информации в корпоративных информационных системах.
5. Приобретение навыка оценки выполнения требований к процессам системы управления информационной безопасностью.
6. Приобретение навыка оценки выполнения требований к организационно-правовому обеспечению применения средств защиты информации.
7. Приобретение навыка оценки выполнения требований по обеспечению защиты информации от вредоносных программ.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы

обучающихся по дисциплине «Безопасность вычислительных систем» 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

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в безопасность вычислительных систем	ПК-2	знает	ПР-7	1-2
			умеет	ПР-6	1-2
			владеет	ПР-6	1-2
2	Раздел II. Безопасность вычислительных систем	ПК-2, ОПК-5	знает	ПР-7	3-16
			умеет	ПР-6	3-16
			владеет	ПР-6	3-16

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. Васильков А.В., Васильков И.А. Безопасность и управление доступом в

информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. — М. : Форум, 2013. — 368 с. — Режим доступа: http://znanium.com/catalog/product/405313

2. Дубинин Е.А., Тебуева Ф.Б., Копытов В.В. Оценка относительного ущерба безопасности информационной системы / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. — М. : РИОР, 2014. — 192 с. — Режим доступа: http://znanium.com/catalog/product/471787

3. Девянин П.Н. Модели безопасности компьютерных систем / П.Н. Девянин — М. : Гор. линия-Телеком, 2012. — 320 с. Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201476.html

Дополнительная литература
(печатные и электронные издания)

1. Нестеренко М.Ю. Информационная безопасность в информационно-вычислительных системах / М.Ю. Нестеренко — Оренбург : ИПК ГОУ ОГУ, 2009. — 107 с. — Режим доступа: https://elibrary.ru/item.asp?id=19593857

2. Гладких А.А. Базовые принципы информационной безопасности вычислительных систем / А.А. Гладких — Ульяновск : Ульяновский государственный технический университет, 2009. — 168 с. — Режим доступа: https://elibrary.ru/item.asp?id=19594481

3. Щербаков А.Ю. Современная компьютерная безопасность / А.Ю. Щербаков — М. : Кн. мир, 2009. — 352 с. — Режим доступа: https://elibrary.ru/item.asp?id=19592342

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Основные положения информационной безопасности: безопасность вычислительных систем [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://studref.com/306318/informatika/bezopasnost_vychislitelnyh_sistem
2. Классификация угроз безопасности распределенных вычислительных систем [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://bugtraq.ru/library/books/attack/chapter03/01.html

Перечень информационных технологий и программного обеспечения

Для выполнения лабораторного задания используется программа Microsoft Word 2010. Для работы с литературой из списка необходимо наличие

у студента аккаунтов в указанных электронно-библиотечной системе: «Znanium.com» (http://znanium.com/), «Консультант студента» (http://www.studentlibrary.ru), «eLIBRARY.RU» (http://elibrary.ru/).

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Безопасность вычислительных систем», 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 (операционная система семейства Windows NT) 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 «Безопасность вычислительных систем»
Направление подготовки 09.03.01 Информатика и вычислительная техника
профиль «Вычислительные машины, комплексы, системы и сети»
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)	25	Отчет о выполнении
2	10-17 неделя обучения	Подготовка лабораторной работы (выполнение отчета к лабораторной работе №2)	38	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 «Безопасность вычислительных систем»
Направление подготовки 09.03.01 Информатика и вычислительная техника
профиль «Вычислительные машины, комплексы, системы и сети»
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	Порядок и методику проведения оценки информационной безопасности; как получать свидетельства оценки и на основе их устанавливать степени выполнения заданных требований по обеспечению информационной безопасности.
	Умеет	Определять основные угрозы информационной безопасности вычислительной системы; осуществлять обоснованный выбор средств и систем защиты информации; реализовывать мероприятия для обеспечения деятельности в области защиты информации.
	Владеет	Навыком формирования требований к средствам защиты информации.
(ПК-2) способность разрабатывать и сопровождать требования к отдельным функциям системы	Знает	Основные требования нормативно-правовой базы информационной безопасности к защите корпоративных информационных систем и их компонентов от несанкционированного доступа к информации, программных средств скрытого информационного воздействия, утечки информации по техническим каналам.
	Умеет	Применять методы определения причин, видов, источников и каналов утечки, искажения информации.
	Владеет	Анализом оценки информационной безопасности и имеет навык устанавливать степени выполнения заданных требований по обеспечению безопасности вычислительной системы.

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 безопасность вычислительных систем	ПК-2	знает	ПР-7	1-2
			умеет	ПР-6	1-2
			владеет	ПР-6	1-2

2	Раздел II. Безопасность вычислительных систем	ПК-2, ОПК-5	знает	ПР-7	3-16
			умеет	ПР-6	3-16
			владеет	ПР-6	3-16

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 информационной безопасности	знает (пороговый уровень)	Порядок и методику проведения оценки информационной безопасности; как получать свидетельства оценки и на основе их устанавливать степени выполнения заданных требований по обеспечению информационной безопасности.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	Определять основные угрозы информационной безопасности вычислительной системы; осуществлять обоснованный выбор средств и систем защиты информации; реализовывать мероприятия для обеспечения деятельности в области защиты информации.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно определять основные угрозы информационной безопасности вычислительной системы, осуществлять обоснованный выбор средств и систем защиты информации самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	владеет (высокий)	Навыком формирования требований к	степень умения отбирать и интегрировать	обучающийся способен самостоятельно сформировать требования

		средствам защиты информации.	имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	к средствам защиты информации.
(ПК-2) способность разрабатывать и сопровождать требования к отдельным функциям системы	знает (пороговый уровень)	Основные требования нормативно-правовой базы информационной безопасности к защите корпоративных информационных систем и их компонентов от несанкционированного доступа к информации, программных средств скрытого информационного воздействия, утечки информации по техническим каналам.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	Применять методы определения причин, видов, источников и каналов утечки, искажения информации.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно применять методы определения причин, видов, источников и каналов утечки, искажения информации самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	владеет (высокий)	Анализом оценки информационной безопасности и имеет навык устанавливать степени выполнения	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя	обучающийся способен самостоятельно провести анализ оценки информационной безопасности и установить степень

		заданных требований по обеспечению безопасности вычислительной системы.	из поставленной цели, проводить самоанализ и самооценку.	выполнения заданных требований по обеспечению безопасности вычислительной системы.

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. Основные определения: информационные системы, вычислительные системы.
2. Безопасность корпоративных информационных систем.
3. Методологии безопасности.
4. Организационно-методологические основы построения защищенных вычислительных систем.
5. Модель нарушителя. Классы нарушителей.
6. Перечень каналов утечки информации.
7. Описание вредоносных воздействий на данные.

8. Классификация методов и средств защиты информации.
9. Инвентаризация методов и средств защиты информации.
10. Анализ степени перекрытия каналов утечки информации.
11. Анализ защищенности данных вычислительных систем.
12. Анализ уязвимости объектов и рисков потери ресурсов.
13. Наиболее распространённые угрозы доступности.
14. Наиболее распространённые угрозы конфиденциальности.
15. Наиболее распространённые угрозы целостности.
16. Оценка показателей объектов зашиты.

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.

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся лабораторные работы. 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.