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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Программно-аппаратные средства обеспечения информационной безопасности
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 5 семестр 9, 10
лекции 36 час.
практические занятия 00 час.
лабораторные работы 72 час.
в том числе с использованием МАО лек. 18 / пр. 00 / лаб. 27 час.
всего часов аудиторной нагрузки 108 час.
в том числе с использованием МАО 45 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 9 семестр
экзамен 10 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 №1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

И. о. заведующего кафедрой : Добржинский Ю.В., к.т.н., с.н.с.
Составитель: Власов А.А.

Владивосток
2019

Оборотная сторона титульного листа РПД

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)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

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

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

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

ABSTRACT

Specialist's degree in *10.05.01 Computer Security*
Specialization "*Mathematical Methods for Information Security*"
Course title: basic scientific research
Basic part of Block 1, *_6_credits 6*
Instructor: Vlasov A.A.
At the beginning of the course a student should be able to:

• • the ability to understand the importance of information in the development of modern society, to apply the achievements of information technologies to search and process information on the profile of activities in global computer networks, library collections and other sources of information (OPK-3);

• ability to use regulatory legal acts in their professional activities (OPK-5);

• the ability to take into account modern trends in the development of computer science and computing technology, computer technology in their professional activities, to work with software tools for general and special purposes (OPK-7);

• the ability to develop formal models of security policies, access control and information flow policies in computer systems, taking into account information security threats (OPK-9);

• ability to analyze and participate in the development of mathematical models of computer system security (PC-4).

Learning outcomes:

- (PC-5) the ability to participate in the development and configuration of software and hardware information security tools, including protected operating systems, database management systems, computer networks, anti-virus protection systems, cryptographic information protection tools
- (PC-16) the ability to develop drafts of regulatory legal acts and methodological materials governing the work on ensuring the information security of computer systems
- (PC-18) the ability to install, adjust, test and maintain modern software and hardware tools to ensure information security of computer systems, including protected operating systems, database management systems, computer networks, anti-virus protection systems, information cryptographic protection

Course description: Discipline has a practical focus, with great importance for the development of the discipline are both laboratory and lecture classes. During the implementation of the discipline in the framework of lectures and laboratory classes, active / interactive training methods are used that implement a visual representation of the results of using software and hardware tools to ensure

information security. The discipline "Software and hardware means of ensuring information security" ensures the acquisition of knowledge and skills in the field of means of ensuring information security using software and hardware. The study of this discipline contributes to the development of fixed assets and methods of protecting information from unauthorized access using hardware and software; requirements of governing documents for the protection of information from unauthorized access.

Main course literature:

1. П.Б. Хорев/. Программно-аппаратная защита информации: учебное пособие - М.: Форум, 2009. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-353-8 - Режим доступа: http://znanium.com/catalog/product/169345

2. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 c.— Режим доступа: http://www.iprbookshop.ru/7000.html

3. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации : учебное пособие для вузов/ С.К. Варлатая, М.В. Шаханова – Владивосток : Изд-во Дальневосточного технического университета, 2007. – 276 с. – Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:386993&theme=FEFU

Form of final control: *pass-fail exam*

Аннотация к рабочей программе дисциплины
«Программно-аппаратные средства обеспечения информационной безопасности»

Рабочая программа «Программно-аппаратные средства обеспечения информационной безопасности» разработана для студентов 5 курса по специальности «Компьютерная безопасность» и входит в состав обязательных дисциплин вариативной части учебного плана с кодом Б1.В.07

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 академических часа. Учебным планом предусмотрены лекционные занятия (36 часа), лабораторные работы (72 часов), самостоятельная работа (54 часов, в том числе 36 часов на подготовку к экзамену). Дисциплина реализуется на 5 курсе, в 9 и 10 семестрах. Форма контроля по дисциплине в 9 семестре – зачет, в 10 семестре – экзамен.

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» основана на предварительном изучении следующих дисциплин: «Информатика», «Основы информационной безопасности», «Модели безопасности компьютерных систем».

Дисциплина имеет практическую направленность, при этом большое значение для освоения дисциплины имеют как лабораторные, так и лекционные занятия. В ходе реализации дисциплины в рамках лекционных и лабораторных занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов использования программно-аппаратных средств обеспечения информационной безопасности. Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» обеспечивает приобретение знаний и умений в области средств обеспечения информационной безопасности программными и аппаратными средствами. Изучение этой дисциплины способствует освоению основных средств и методов защиты информации от несанкционированного доступа с использованием аппаратно-программных средств; требований руководящих документов по защите информации от

несанкционированного доступа.

Цель дисциплины: сформировать представление о проблемах защиты информации в автоматизированных системах обработки информации; раскрыть природу явлений, заключающихся в нарушении целостности и конфиденциальности информации и дезорганизации работы компьютерных сетей;

Задачи:

- изучить требования руководящих документов по защите информации от несанкционированного доступа (НСД);
- изучить систему защиты информации от НСД;
- устанавливать, переустанавливать, удалять системы защиты информации;
- настраивать защитные механизмы систем защиты информации;
- составлять правила фильтрации криптомаршрутизатора.

Для успешного изучения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);
- способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения(ОПК-7);

• способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);

• способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем(ПК-4).

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПК-5) способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	особенности каналов утечки информации в компьютерных системах, методы и технические перекрытия этих каналов.
	Умеет	анализировать каналы утечки информации, возможные в конкретной компьютерной системе, организовывать защиту информации в ней.
	Владеет	программными и техническими средствами защиты информации в компьютерных системах.
(ПК-16) способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	Знает	организационные, программные и технические методы защиты информации.
	Умеет	анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным реальным условиям. составлять проекты нормативных правовых актов по комплексной защите информации.
	Владеет	методами и навыками анализа создания систем защиты информации.
(ПК-18) способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной	Знает	методы технической и программной защиты информации.

безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Умеет	тестировать конкретные компьютерные системы с использованием аппаратных и программных средств на предмет уровня защищённости информации в них и в помещениях, где они расположены.
	Владеет	программными и аппаратными средствами контроля защиты информации

Для формирования вышеуказанных компетенций в рамках дисциплины применяются следующие методы обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспект (ПР-7), лабораторные работы (ПР-6).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА - лекции (72 час.)

Раздел 1.«Secret Net» - (9 час)

Тема 1. Требования руководящих документов по защите информации от НСД

Тема 2. Классификация программно-аппаратных средств защиты информации. Подсистема доверенной загрузки ОС. Краткая характеристика средств защиты информации от НСД

Тема 3. Система защиты информации «Secret Net». История развития. Архитектура и характеристика основных компонентов. Механизмы защиты

Тема 4. Программно-аппаратный комплекс защиты информации от НСД «Соболь».

Раздел 2.«ViPNet Client 3.2 КС3» - (42 час)

Тема 1. Состав программных средств ПК «ViPNet Client КС3»

Основные принципы функционирования

Требования к составу технических средств и операционным системам

Дополнительное программное обеспечение

Тема 2. Разграничение полномочий в сети ViPNet.

Группа администраторов безопасности

Группа администраторов ЦУС

Группа администраторов УКЦ

Тема 3. Требования к размещению технических средств.

Тема 4. Установка и ввод в эксплуатацию ПК «ViPNet Client КС3».

Установка ПК «ViPNet Client КС3»

Ввод в эксплуатацию

Требования к настройкам ПК «ViPNet Client КС3»

Регистрация пользователей и СУ в сети ViPNet

Тема 5. Эксплуатация ПК «ViPNet Client КС3».

Контроль целостности ТС и ПО

Контроль работоспособности и соблюдения правил эксплуатации

Обновление ПО «ViPNet Client КС3»

Восстановление работоспособности при сбоях

Тема 6. Организационно-технические и административные мероприятия по

защите от несанкционированного доступа при использовании ПК «ViPNet Client КС3»

Общие положения
Организация работ по защите от НСД
Требования по защите от НСД при эксплуатации ПК «ViPNet Client КС3»
Настройка правил фильтрации
Экспорт/импорт списка правил фильтрации

Тема 7. Ключевая информация.
Состав ключевой информации, аутентификация
Требования по хранению ключевой информации
Удаление ключевой информации
Плановая смена и обновление ключевой информации
Компрометация ключевой информации, смена ключей при компрометации

Раздел 3. «Dallas Lock 8.0-C» - (4 час)

Тема 1. Установка и ввод в эксплуатацию «Dallas Lock 8.0-C»
Основные принципы функционирования
Установка «Dallas Lock 8.0-C»
Ввод в эксплуатацию «Dallas Lock 8.0-C»
Требования к настройкам «Dallas Lock 8.0-C»

Раздел 4. «Security Studio Endpoint Protection» - (4 час)

Тема 1. Установка и ввод в эксплуатацию «Security Studio Endpoint Protection» - 4 час.

Основные принципы функционирования
Установка «Security Studio Endpoint Protection»
Ввод в эксплуатацию «Security Studio Endpoint Protection»
Требования к настройкам «Security Studio Endpoint Protection»

Раздел 5.«Kaspersky Endpoint Security 10 для Windows» (4 час)

Тема 1. Установка и ввод в эксплуатацию «Kaspersky Endpoint Security 10 для Windows»
Основные принципы функционирования
Установка «Kaspersky Endpoint Security 10 для Windows»
Ввод в эксплуатацию «Kaspersky Endpoint Security 10 для Windows»
Требования к настройкам «Kaspersky Endpoint Security 10 для Windows»

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (90 час.)

Лабораторная работа №1. Материально-техническое обеспечение практических занятий. Программно-аппаратные средства, программное обеспечение. Автоматизированные рабочие места. **(10 час.)**

Лабораторная работа №2. Установка программного обеспечения ПАК «Соболь». Инициализация платы, перевод в рабочий режим. Настройка системы. Подготовка идентификаторов для пользователей. Настройка механизмов защиты. Режим интеграции с «Secret Net **(10 час.)**

Лабораторная работа №3. Установка, исправление, удаление программного обеспечения для Windows-XP. Особенности установки. Режим интеграции с ПАК «Соболь». Временное отключение защитных механизмов **(10 час.)**

Лабораторная работа №4. Настройка механизма защиты входа в систему. Подготовка идентификаторов пользователю. Настройка режимов «Вход и администрирование ПАК «Соболь», «Вход в систему по идентификаторам», «Режим усиленной идентификации» **(10 час.)**

Лабораторная работа №5. Настройка механизма избирательного доступа к устройствам. Настройка механизма контроля аппаратной конфигурации **(20 час.)**

Лабораторная работа №6. Настройка механизма полномочного разграничения доступа.

Лабораторная работа №7. Настройка механизма шифрования Настройка механизма контроля целостности и замкнутой программной среды Тема 8. Механизм регистрации событий. Дополнительные механизмы защиты. Формирование отчетов. Импорт и экспорт настроек системы защиты - 1 час**.(20 час.)**

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Математическая логика и теория алгоритмов» 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	
				текущий контроль	промежуточная аттестация
1	Раздел I.	ПК-5 ПК-5 ПК-5	знает	конспект (ПР-7),	1-4
			умеет	лабораторные работы (ПР-6).	1-4
			владеет	конспект (ПР-7),	1-4
2	Раздел II.	ПК-5 ПК-5 ПК-5	знает	конспект (ПР-7),	5-10
			умеет	лабораторные работы (ПР-6).	5-10
			владеет	конспект (ПР-7),	5-10
3	Раздел III.	ПК-5	знает	конспект	11-20

		ПК-5 ПК-5		(ПР-7),	
			умеет	лабораторные работы (ПР-6).	11-20
			владеет	конспект (ПР-7),	11-20

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО

Основная литература

1. П.Б. Хорев/. Программно-аппаратная защита информации: учебное пособие - М.: Форум, 2009. - 352 с.: ил.; 60х90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-353-8 - Режим доступа: http://znanium.com/catalog/product/169345

2. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: http://www.iprbookshop.ru/7000.html

3. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации : учебное пособие для вузов/ С.К. Варлатая, М.В. Шаханова – Владивосток : Изд-во Дальневосточного технического университета, 2007. – 276 с. – Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:386993&theme=FEFU

Дополнительная литература

1. Помешкин А.А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс]: учебно-методическое пособие/ Помешкин А.А., Коротких И.В.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2012.— 47 с.— Режим доступа: http://www.iprbookshop.ru/45015.html

2. Соколов В.П. Кодирование в системах защиты информации [Электронный ресурс]: учебное пособие/ Соколов В.П., Тарасова Н.П.— Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2016.— 94 с.— Режим доступа: http://www.iprbookshop.ru/61485.html

3. Ключев А.О., Ковязина Д.Р., Кустарев П.В., Платунов А.Е. Аппаратные и программные средства встраиваемых систем [Электронный ресурс]: учебное пособие/ А.О. Ключев [и др.].— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2010.— 291 с.— Режим доступа: http://www.iprbookshop.ru/65790.html

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ДИСЦИПЛИНЫ

Технические средства, используемые для отработки практических вопросов дисциплины:

- две виртуальные машины, на которых настроены СЗИ «Dallas Lock 8.0-C», «Kaspersky Endpoint Security 10 для Windows», «Security Studio Endpoint Protection» и программный комплекс «ViPNet Client 3.2 КС3»;
- 6 персональных компьютеров, которые объединены в две подсети с серверами безопасности;

- Программно- аппаратный комплекс «Соболь»

- Система защиты информации «Secret Net» с аппаратной поддержкой - платой «Соболь»

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь, монитор 17"" Aser-173 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 "

Приложение 1

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

Специальность 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-17 недели обучения	Подготовка лабораторной работы №1 (выполнение отчета к лабораторной работе №1)	28	Отчеты о выполнении лабораторной работы
2	18 неделя обучения	Подготовка к зачету	8	Зачет
3	19-36 недели обучения	Подготовка лабораторной работы №2 (выполнение отчета к лабораторной работе №2)	28	Отчеты о выполнении лабораторной работы
4	Сессия	Подготовка к экзамену	54	Экзамен

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

Приложение 2

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

Специальность 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-5) способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	Особенности каналов утечки информации в компьютерных системах, методы и технические перекрытия этих каналов.
	Умеет	Анализировать каналы утечки информации, возможные в конкретной компьютерной системе, организовывать защиту информации в ней.
	Владеет	Программными и техническими средствами защиты информации в компьютерных системах.
(ПК-16) способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	Знает	Организационные, программные и технические методы защиты информации.
	Умеет	Анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным реальным условиям. Составлять проекты нормативных правовых актов по комплексной защите информации.
	Владеет	Методами и навыками анализа создания систем защиты информации.
(ПК-18) способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных	Знает	Методы технической и программной защиты информации.
	Умеет	Тестировать конкретные компьютерные системы с использованием аппаратных и программных средств на предмет уровня защищённости информации в них и в помещениях, где они расположены.
	Владеет	Программными и аппаратными средствами контроля защиты информации

систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I.	ПК-5 ПК-5 ПК-5	знает	конспект (ПР-7),	1-4
			умеет	лабораторные работы (ПР-6).	1-4
			владеет	конспект (ПР-7),	1-4
2	Раздел II.	ПК-5 ПК-5 ПК-5	знает	конспект (ПР-7),	5-10
			умеет	лабораторные работы (ПР-6).	5-10
			владеет	конспект (ПР-7),	5-10
3	Раздел III.	ПК-5 ПК-5 ПК-5	знает	конспект (ПР-7),	11-20
			умеет	лабораторные работы (ПР-6).	11-20
			владеет	конспект (ПР-7),	11-20

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачет и экзамен.

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

Зачет и экзамен проводится в форме собеседования (УО-1), вопросы к зачету и экзамену соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. Для подготовки к ответу на зачете и экзамене 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:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.
- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для промежуточной аттестации

Список вопросов на зачет

1. Требования руководящих документов по защите информации от НСД.
2. Классификация программно-аппаратных средств защиты информации.
3. Подсистема доверенной загрузки ОС.
4. Краткая характеристика средств защиты информации от НСД.
5. Система защиты информации «Secret Net». История развития. Архитектура и характеристика основных компонентов. Механизмы защиты.

6. Программно-аппаратный комплекс защиты информации от НСД «Соболь».

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.

Список вопросов на экзамен

1. Состав комплекса «Континент-К».
2. Основные принципы функционирования комплекса.
3. Возможности и достоинства АПК «КОНТИНЕНТ-К».
4. Организация удаленного доступа.
5. Фильтрация трафика для удаленного доступа.

Каждый экзаменационный билет содержит два вопроса из списка выше. Результаты экзамена оцениваются по четырёхбалльной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и заносятся в

экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, сведениям из информационных ресурсов Интернет.

Оценка **«отлично».** Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания дисциплины. Соблюдаются нормы литературной речи.

Оценка **«хорошо».** Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.

Оценка **«удовлетворительно».** Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.

Оценка **«неудовлетворительно».** Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.

В случае неявки студента на экзамен в экзаменационной ведомости делается отметка «не явился».

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.

Приложение 3

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

Специальность 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток
2019

Количество аудиторных часов, отведенных на изучение дисциплины «Программно-аппаратные средства обеспечения информационной безопасности», составляет 134 часа. На самостоятельную работу студента отведено 64 часов, в том числе 54 часов на подготовку к экзамену.

Аудиторная нагрузка состоит из 46 часов лекционных занятий и 88 часов, отведённых на лабораторные работы. 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.

При подготовке к лабораторным занятиям также необходимо повторить теоретический материал. Лабораторные работы представляют собой задания различного типа, направленные на получение обучающимся практических знаний по теме. 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.

Промежуточная форма аттестации по данной дисциплине – зачет и экзамен. Вопросы к зачету и экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к зачету и экзамену студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.