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 _54__ час.
практические занятия___00____час.
лабораторные работы___90____час.
в том числе с использованием МАО лек.__18___/пр.___00__/лаб.___6__ час.
в том числе в электронной форме лек.__00___/пр.__00___/лаб.___00__ час.
всего часов аудиторной нагрузки____144____ час.
в том числе с использованием МАО __24___ час.
в том числе в электронной форме __00__ час.
самостоятельная работа _____108____ час.
в том числе на подготовку к экзамену ___36___ час.
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 (ли): Власов А.А. Ст преп.

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: *Software and hardware information security*

Basic part of Block 1, _7_credits

Instructor: *Vlasov A.A.*

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

• the ability to understand the value of information in the development of modern society, to apply the achievements of information technology to search and process (OPK-3);

• ability to apply research methods in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4);

• 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. *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*

2. *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*

3. *Объектно-ориентированное программирование с примерами на C#: Учебное пособие / Хорев П.Б. - М.: Форум, НИЦ ИНФРА-М, 2016. - 200 с.: 70x100 1/16. - (Высшее образование: Бакалавриат) (Обложка) ISBN 978-5-00091-144-0 - Режим доступа: http://znanium.com/catalog/product/529350*

4. *Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса "Secret Net 5.0" / Помешкин А.А., Коротких И.В. - Новосиб.:НГТУ, 2012. - 47 с.: ISBN 978-5-7782-1990-8 - Режим доступа: http://znanium.com/catalog/product/556699*

Form of final control: *exam, pass-fail exam*

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

Курс учебной дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» разработан для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит обязательные дисциплины вариативной части дисциплин учебного плана Б1.В.ОД.8.

Общая трудоемкость освоения дисциплины составляет 7 зачетных единицы, 252 часа. Учебным планом предусмотрены лекционные занятия (54 часа), лабораторные работы (90 часа), самостоятельная работа (108 час, в том числе 36 час на подготовку к экзамену). Дисциплина реализуется на 5 курсе, в 9 и 10 (А) семестрах. Форма контроля по дисциплине – зачёт в 9 семестре, экзамен в 10 (А) семестре.

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

безопасности», «Модели безопасности компьютерных систем», «Аппаратные средства вычислительной техники».

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: 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; выработать умения и навыки применять основные методы и приемы защиты информации в автоматизированных системах, используя системы защиты информации и криптомаршрутизаторы.

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 (ОПК-3);
- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- 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).
- способностью 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	**Этапы формирования компетенции**

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 систем, включая защищенные операционные системы, системы управления базами данных,	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.

компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		

Для формирования вышеуказанных компетенций в рамках дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7), лабораторные работы (ПР-6).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Вводный (24 час.)

«Secret Net» - (10 час) – 9 семестр

Тема 1. Требования руководящих документов по защите информации от НСД - 6 час.

Тема 2. Классификация программно-аппаратных средств защиты информации. Подсистема доверенной загрузки ОС. Краткая характеристика средств защиты информации от НСД - 4 час.

Тема 3. Система защиты информации «Secret Net». История развития. Архитектура и характеристика основных компонентов. Механизмы защиты – 6 час.

Тема 4. Программно-аппаратный комплекс защиты информации от НСД «Соболь» - 2 час.

«ViPNet Client 3.2 КС3» - (14 час) – 10 семестр

Тема 1. Состав программных средств ПК «ViPNet Client КС3» - 6 час.

Основные принципы функционирования
Требования к составу технических средств и операционным системам
Дополнительное программное обеспечение

Тема 2. Разграничение полномочий в сети ViPNet - 6 час.

Группа администраторов безопасности
Группа администраторов ЦУС
Группа администраторов УКЦ

Тема 3. Требования к размещению технических средств - 6 час.

Тема 4. Установка и ввод в эксплуатацию ПК «ViPNet Client КС3» - 6 час.

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» - 6 час.

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» - 6 час.

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 - 6 час.

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 II. Основной (30 час.)

«Dallas Lock 8.0-C» - (10 час) – 10 семестр

Тема 1. Установка и ввод в эксплуатацию «Dallas Lock 8.0-C» - 4 час.

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»

«Security Studio Endpoint Protection» - (10 час) – 10 семестр

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»

«Kaspersky Endpoint Security 10 для Windows» (10 час) – 10 семестр

Тема 1. Установка и ввод в эксплуатацию «Kaspersky Endpoint Security 10 для Windows» - 4 час.

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.)

«Secret Net» (36 час):

Лабораторная работа:

Тема 1. 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» - 4 час.

Тема 2. Установка, исправление, удаление программного обеспечения для Windows-XP. Особенности установки. Режим интеграции с ПАК «Соболь». Временное отключение защитных механизмов – 4 час

Тема 3. Настройка механизма защиты входа в систему. Подготовка идентификаторов пользователю. Настройка режимов «Вход и администрирование ПАК «Соболь», «Вход в систему по идентификаторам», «Режим усиленной идентификации» - 4 час

Тема 4. Настройка механизма избирательного доступа к устройствам. Настройка механизма контроля аппаратной конфигурации – 4 час.

Тема 5. Настройка механизма полномочного разграничения доступа – 8 час.

Тема 6. Настройка механизма шифрования – 4 час.

Тема 7. Настройка механизма контроля целостности и замкнутой программной среды – 4 час.

Тема 8. Механизм регистрации событий. Дополнительные механизмы защиты. Формирование отчетов. Импорт и экспорт настроек системы защиты - 4 час.

«ViPNet Client 3.2 КС3» - (24 час.)

Занятие 1. Ввод комплекса в эксплуатацию - 6час.

Установка ПК «ViPNet Client КС3»
Ввод в эксплуатацию
Требования к настройкам ПК «ViPNet Client КС3»

Регистрация пользователей и СУ в сети ViPNet

Занятие 2. Эксплуатация ПК ViPNet Client КС3 - 6 час.

Контроль целостности ТС и ПО
Контроль работоспособности и соблюдения правил эксплуатации
Обновление ПО «ViPNet Client КС3»
Восстановление работоспособности при сбоях

Занятие 3. Ключевая информация - 6 час.

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

Занятие 4.Настройка программы «Деловая почта» - 6 час.

Определение доступности узлов
Настройка шифрования и подписания отправляемых пакетов
Настройка автопроцессинга
Определение статуса отправленных пакетов
Транспортный модуль MFTP

«Dallas Lock 8.0-C» - (10 час)

Занятие 1. Ввод комплекса в эксплуатацию – 10 час.

Установка «Dallas Lock 8.0-C»С3
Ввод в эксплуатацию
Требования к настройкам «Dallas Lock 8.0-C»

«Security Studio Endpoint Protection» - (10 час)

Занятие 1. Ввод комплекса в эксплуатацию – 10 час.

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

«Kaspersky Endpoint Security 10 для Windows»- (10 час)

Занятие 1. Ввод комплекса в эксплуатацию – 10 час.

Установка «Kaspersky Endpoint Security 10 для Windows»
Ввод в эксплуатацию
Требования к настройкам «Kaspersky Endpoint Security 10 для Windows»

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Основная литература и электронные ресурсы

Вся документация на ПК «ViPNet Client 3.2 КС3» может быть найдена на сайте ОАО «ИнфоТеКС» http://infotecs.ru:

1. ViPNet_Client_КС3_Ru.pdf
2. ViPNet_Deployment_Ru.pdf
3. ViPNet_MFTP_Ru.pdf
4. П.Б. Хорев. Методы и средства защиты информации в компьютерных системах: учебное пособие.-М.: Академия, 2006. 256 с.
5. Комплект нормативных документов: Федеральные законы, Госстандарты, Руководящие документы.
6. Программно-аппаратный комплекс «Соболь PCI». УВАЛ.00300-26 91. ЗАО НИП «ИНФОРМЗАЩИТА», 2001. 76 с.

8. Система защиты информации Secret Net (автономный вариант). Описание системы. Руководство администратора УВАЛ. 00300-107 91 1

9. Система защиты информации Secret Net (автономный вариант). Управление. Основные механизмы защиты. Руководство администратора УВАЛ. 00300-107 91 2

10. Система защиты информации Secret Net (автономный вариант). Управление. Полномочное разграничение доступа. Руководство администратора УВАЛ. 00300-107 91 3

11. Система защиты информации Secret Net (автономный вариант).

Аудит. Руководство администратора УВАЛ. 00300-107 91 4

12. Система защиты информации Secret Net . Аппаратные средства. Руководство администратора УВАЛ. 00300-106 91 9

13. Система защиты информации Secret Net . Руководство пользователя УВАЛ. 00300-106 92

14. ViPNet Administrator Центр управления сетью. Руководство администратора, ОАО «ИнфоТеКС», ФРКЕ.00006-05 32 01.

15. ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора, ОАО «ИнфоТеКС», ФРКЕ.00101-05 32 02.

16. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.

17. ViPNet Client Монитор 3.2. Руководство пользователя, ОАО «ИнфоТеКС», ФРКЕ.00063-05 34 01.

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. Вводный	ПК-5, ПК-16, ПК-18	знает	Конспект (ПР-7)	1-6
			умеет	Лабораторная работа (ПР-6)	1-6
			владеет	Лабораторная работа (ПР-6)	1-6
2	Раздел II. Основной	ПК-5, ПК-16, ПК-18	знает	Конспект (ПР-7)	7-11
			умеет	Лабораторная работа (ПР-6)	7-11
			владеет	Лабораторная работа (ПР-6)	7-11

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА

1. 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

2. 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

3. Объектно-ориентированное программирование с примерами на C#: Учебное пособие / Хорев П.Б. - М.: Форум, НИЦ ИНФРА-М, 2016. - 200 с.: 70x100 1/16. - (Высшее образование: Бакалавриат) (Обложка) ISBN 978-5-00091-144-0 - Режим доступа: http://znanium.com/catalog/product/529350

4. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса "Secret Net 5.0" / Помешкин А.А., Коротких И.В. - Новосиб.:НГТУ, 2012. - 47 с.: ISBN 978-5-7782-1990-8 - Режим доступа: http://znanium.com/catalog/product/556699

Дополнительная литература

1. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс]: учебное пособие для вузов/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный

технический университет, 2012.— 224 с.— Режим доступа: http://www.iprbookshop.ru/7007.html
2. Аверченков, В.И. Система обеспечения безопасности Российской Федерации : учеб. пособие / В.И. Аверченков, В.В. Ерохин; Брянский гос. техн. ун-т. — Брянск : Изд-во Брянского технического университета, 2005. — 120 с. — Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:384623&theme=FEFU
3. Платонов, В.В. Программно-аппаратные средства защиты информации : учебник для вузов / В.В. Платонов. — Москва : Академия, 2014. — 331 с. — Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:790443&theme=FEFU

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 549 Компьютерный класс, 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: "Моноблок lenovo C360G-i34164G500UDK Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Aversion CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор, Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718" Доска аудиторная

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, 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: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: 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 Доска аудиторная

I. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения лекционных и лабораторных занятий необходима аудитория с мультимедиа проектором и экраном. Лабораторные работы выполняются в аудитории, оборудованной компьютерами и доступом в сеть «Интернет». Количество рабочих мест в аудитории должно соответствовать количеству обучающихся. Для самостоятельной работы (использование ЭБС) студенту также необходим компьютер и доступ в сеть «Интернет».

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»

Направление подготовки 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	1-18 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	36	Отчет о выполнении практического задания
2	Сессия	Подготовка и сдача экзамена	36	Экзамен

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-17 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	18	Отчет о выполнении практического задания
2	18 неделя обучения	Подготовка и сдача зачета	18	Зачет

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения **«зачтено»** отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка **«незачтено»** выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.

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»

Направление подготовки 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	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.

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

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Вводный	ПК-5, ПК-16, ПК-18	знает	Конспект (ПР-7)	1-6
			умеет	Лабораторная работа (ПР-6)	1-6
			владеет	Лабораторная работа (ПР-6)	1-6
2	Раздел II. Основной	ПК-5, ПК-16, ПК-18	знает	Конспект (ПР-7)	7-11
			умеет	Лабораторная работа (ПР-6)	7-11
			владеет	Лабораторная работа (ПР-6)	7-11

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».

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.

Критерии выставления оценки на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только

	основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

6.

Критерии выставления оценки на зачет

Оценка	Требования к сформированным компетенциям
«зачтено»	Оценка «зачтено» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«не зачтено»	Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
3	ПР-6	Лабораторная работа	Средство для закрепления и практического освоения материала по определенному разделу	Комплект лабораторных заданий
4	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины