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

ИНЖЕНЕРНАЯ ШКОЛА

«СОГЛАСОВАНО»
Руководитель ОП
«Вычислительные машины, комплексы и компьютерные сети»

_____ Доброжинский Ю.В.
(подпись) (Ф.И.О. рук. ОП)
«01» февраля 2020 г.

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Корнюшин П.Н.
(подпись) (Ф.И.О. зав. каф.)
«01» февраля 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Комплексная безопасность вычислительных систем

Направление подготовки 09.06.01 Информатика и вычислительная техника
профиль «Вычислительные машины, комплексы и компьютерные сети»
Форма подготовки очная

курс ___2___ семестр ___3___
лекции _8_ час.
практические занятия__10___час.
лабораторные работы_____час.
в том числе с использованием МАО лек.__6__/пр.__8__/лаб._____ час.
всего часов аудиторной нагрузки___18___ час.
в том числе с использованием МАО _14_ час.
самостоятельная работа ___126____ час.
в том числе на подготовку к экзамену __18__ час.
контрольные работы (количество)
курсовая работа / курсовой проект _____ семестр
зачет _____ семестр
экзамен____3_____семестр

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 30.07.2014 № 875

Рабочая программа обсуждена на заседании кафедры информационной безопасности, протокол № 5 от «01» февраля 2020 г.

И.о. зав. кафедрой Корнюшин П.Н., д.ф.-м.н., профессор
Составитель: Варлатая С.К., к.т.н., доцент

Оборотная сторона титульного листа РПУД

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

Degree in 09.06.01 Computer science and engineering

Study profile: Computers, complexes and computer networks

Course title: *Complex Security of Computing Systems*

Variable part of Block 1, 4 credits

Instructor: Varlataya S.K.

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

- possession of methods for conducting patent research, licensing and copyright protection in the creation of innovative products in the field of professional activity (GPC-7);

- the ability to create algorithms, methods, software and hardware tools that provide increased reliability, quality control, fault tolerance and diagnostics of the functioning of computing systems and their components (PC-4);

- readiness to participate in the work of Russian and international research teams to solve scientific and scientific-educational tasks (UC-3).

Learning outcomes:

- readiness for teaching activity in basic educational programs of higher education (GPC-8);

- the ability to perform theoretical analysis and experimental studies of the functioning of computers, complexes and computer networks in order to improve the characteristics of their functionality and integrated security (PC-1);

- readiness to use modern methods and technologies of scientific communication in the state and foreign languages (UC-4);

- the ability to plan and solve problems of their own professional and personal development (UC-6).

Course description: The content of the discipline covers the following issues: security methods, types of threats, security models and their application, cryptographic methods of information protection, protection of operating systems from unauthorized access.

Main course literature:

1. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс - Москва : Проспект, 2015. – 216 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:791193&theme=FEFU

2. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова – М. : Проспект, 2015. – 152 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:791159&theme=FEFU

3. В. Ф. Шаньгин Комплексная защита информации в корпоративных системах : учебное пособие для вузов. Москва : Форум, : Инфра-М, 2015. – 591 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:294516&theme=FEFU

4. В. В. Платонов Программно-аппаратные средства защиты информации : учебник для вузов / Москва : Академия, 2014. – 331 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:790443&theme=FEFU

5. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / М.А. Иванов, И.В. Чугунков. — Электрон. дан. — Москва : НИЯУ МИФИ, 2012. — 400 с. — Режим доступа: https://e.lanbook.com/book/75810

Form of final control: exam.

Аннотация к рабочей программе дисциплины
«Комплексная безопасность вычислительных систем»

Курс учебной дисциплины «Комплексная безопасность вычислительных систем» предназначен для обучения аспирантов по направлению 09.06.01 «Информатика и вычислительная техника», профиль «Вычислительные машины, комплексы и компьютерные сети» и входит в состав обязательных дисциплин вариативной части учебного плана Б1.В.ОД.4.

Общая трудоемкость освоения дисциплины составляет 144 часов (4 з.е.). Учебным планом предусмотрены лекционные занятия (8 час.), практические занятия (10 час.), самостоятельная работа (108 час.), подготовка к экзамену (18 час.). Дисциплина реализуется на 2 курсе в 3 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Комплексная безопасность вычислительных систем» логически и содержательно связана с такими курсами, как «Тестирование и диагностика вычислительных систем», «Вычислительные машины, комплексы и компьютерные сети».

Содержание дисциплины охватывает следующий круг вопросов: методы обеспечения безопасности, виды угроз, модели безопасности и их применение, криптографические методы защиты информации, защита операционных систем от несанкционированного доступа.

Цель изучения дисциплины «Комплексная безопасность вычислительных систем» заключаются в освоении методов, средств и тенденций развития обеспечения безопасности вычислительных систем.

Задачи:

- формирование знаний об основных принципах построения системы защиты вычислительных систем различной архитектуры;
- изучение системного подхода к проблеме защиты информации в вычислительных системах;
- формирование знаний о современных методах и способах защиты информации;
- изучение основ проектирования систем обеспечения безопасности.

Для успешного изучения дисциплины «Комплексная безопасность вычислительных систем» у обучающихся должны быть сформированы следующие предварительные компетенции (элементы компетенций):

- владение методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности (ОПК-7);

- способность создавать алгоритмы, методы, программно-аппаратные средства, обеспечивающие повышение надежности, качества контроля, отказоустойчивости и диагностики функционирования вычислительных систем и их компонент (ПК-4);

- готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач (УК-3).

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

Код и формулировка компетентности	**Этапы формирования компетентности**	
ОПК-8 – готовность к преподавательской деятельности по основным образовательным программам высшего образования	Знает	основные требования к организации преподавательской деятельности
	Умеет	оценивать текущее состояние и тенденции развития образовательных программ в области информационных исследований
	Владеет	способами и демонстрации умения представлять результаты исследований
ПК-1 – способность выполнять теоретический анализ и экспериментальные исследования функционирования вычислительных машин, комплексов и компьютерных сетей с целью улучшения характеристик их функциональности и комплексной безопасности	Знает	основные требования к организации теоретических и экспериментальных исследований компьютерной техники
	Умеет	осуществлять отбор и использовать оптимальные сочетания теоретических и экспериментальных исследований
	Владеет	методами теоретических исследований обеспечения функциональности и безопасности вычислительных систем
УК-4 – готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	Знает	методы и технологии научной коммуникации на государственном и иностранном языках
	Умеет	следовать основным нормам, принятым в научном общении на государственном и иностранном языках
	Владеет	различными методами, технологиями и типами коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках
УК-6 – способность планировать и решать задачи собственного профессионального и личностного развития	Знает	содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда
	Умеет	формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессио-

		нальной деятельности, этапов профессионального роста, индивидуально-личностных особенностей
	Владеет	способами выявления и оценки индивидуально-личностных, профессионально-значимых качеств и путями достижения более высокого уровня их развития

Для формирования вышеуказанных компетенций в рамках дисциплины «Комплексная безопасность вычислительных систем» 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).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Базовые задачи и методы обеспечения безопасности (2 час.)

Тема 1. Введение, задачи и содержание курса (1 час).

Задачи и содержание курса, порядок его изучения. Материально-техническая и учебно-методическая база. Изучение основных понятий и определений, используемых при изучении дисциплины. Международные стандарты информационного обмена. Получение статистических знаний об атаках, которым подвергаются компьютерные системы.

Тема 2. Современные методы защиты информации (1 часа).

Основные технологии построения защищенных ИС. Место информационной безопасности в национальной безопасности страны. Концепция информационной безопасности.

Проблемные вопросы: Ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Internet.

Раздел II. Угрозы и вирусы (2 час.)

Тема 1. Виды угроз, нарушений, противников (1 час).

Понятие угрозы. Три вида возможных нарушений информационной системы. Виды противников или «нарушителей». Информационная безопасность в условиях функционирования в России глобальных сетей.

Проблемные вопросы: Получение знаний о видах угроз, путей и каналов утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками.

Тема 2. Вирусы и защита от них (1 час).

Понятия о видах вирусов. Получение знаний о существующих "компьютерных вирусах". Классификация "компьютерных вирусов". Основные правила защиты от "компьютерных вирусов". Обзор антивирусных программ. Методика использования антивирусных программ. Восстановление пораженных "компьютерными вирусами" объектов.

Раздел III. Формализация задач обеспечения безопасности вычислительных систем (2 час.)

Тема 1. Модели безопасности и их применение (1 час).

Дискреционная и мандатная модели политики безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.

Тема 2. Методы криптографии (1 час).

Традиционные и современные криптосистемы. Методы шифрования данных. Основные криптографические алгоритмы. Абонентское и пакетное шифрование. Взаимное подтверждение подлинности (аутентификация) абонентов и объектов сети. Обеспечение целостности информации на основе электронной цифровой подписи.

Лекция-пресс-конференция

В начале занятия преподаватель называет тему лекции и просит студентов письменно задавать ему вопросы по данной теме. Каждый аспирант должен в течение 2-3 минут сформулировать наиболее интересующие его вопросы по теме лекции, написать их на листке бумаги и передать записку преподавателю. Преподаватель в течение 3-5 минут сортирует вопросы по их смысловому содержанию и начинает читать лекцию. Изложение материала преподносится в виде связного раскрытия темы, а не как ответ на каждый заданный вопрос, но в процессе лекции формулируются соответствующие ответы. В завершение лекции преподаватель проводит итоговую оценку вопросов, выявляя знания и интересы аспирантов.

Раздел IV. Защита операционных систем (2 час.)

Тема 1. Методы несанкционированного доступа к операционным системам (1 час).

Основные механизмы функционирования ОС. Основные термины безопасности ОС. Разграничение доступа к ОС.

Тема 2. Основные механизмы защиты в операционных системах Linux и Windows (1 час).

Пользователи и группы в Linux. Разделение доступа. Системы мандатной защиты. SELinux. Защита ОС в сети. Сетевые экраны. IPTables.

Пользователи и группы в Windows. Разделение доступа. Брандмауэр Windows. Защита ОС в сети. Защита в Active Directory.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (10 час.)

Занятие 1. Решение задач обеспечения безопасности предприятия. (3 час.)

1. Построение политики безопасности предприятия.
2. Назначение паролей и логинов
3. Проверка в системе аутентификации.

Занятие 2. Решение задач эффективного кодирования. (3 час.)

1. Симметричное кодирование.
2. Асимметричное кодирование.
3. Электронно – цифровая подпись.

Диспут. Понятие шифрования данных. Шифрования уровня отдельных файлов. Шифрование на уровне файловой системы. Сертификаты и ключи. Резервное копирование. Снимки файловых систем. Журналирование

Занятие 3. Решение задач обеспечения безопасности операционных систем. (4 час.)

1. Установка операционных систем Linux и Windows на виртуальную машину.
2. Базовая настройка основных систем безопасности ОС.
3. Получение несанкционированного доступа с использованием уязвимости ОС.
4. Организация виртуальной среды на основе технологии LXC.
5. Создание и администрирование пользователей.

Проблемные вопросы. Отображение и смена SID. Генерация SID. Фильтрация трафика средствами Windows. Резервирование и восстановление целостности в Active Directory.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Тестирование и диагностика 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	
				текущий контроль	промежуточная аттестация
1	Раздел I. Базовые задачи и методы обеспечения безопасности	ОПК-8, ПК-1, УК-4, УК-6	знает	собеседование (ОУ-1)	1-5
			умеет	коллоквиум (ОУ-2)	1-5
			владеет	конспект (ПР-7)	1-5
2	Раздел II. Угрозы и вирусы	ОПК-8, ПК-1, УК-4, УК-6	знает	собеседование (ОУ-1)	6-10
			умеет	коллоквиум (ОУ-2)	6-10
			владеет	конспект (ПР-7), отчет о выполнении практического задания	6-10
3	Раздел III. Формализация задач обеспечения безопасности вычислительных систем	ОПК-8, ПК-1, УК-4, УК-6	знает	собеседование (ОУ-1)	11-21
			умеет	коллоквиум (ОУ-2)	11-21
			владеет	конспект (ПР-7), отчет о выполнении практического задания	11-21
4	Раздел IV. Защита	ОПК-8,	знает	собеседование	22-30

	операционных систем	ПК-1, УК-4, УК-6		(ОУ-1)	
			умеет	коллоквиум (ОУ-2)	22-30
			владеет	конспект (ПР-7), отчет о выполнении практического задания	22-30

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(печатные и электронные издания)

1. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс - Москва : Проспект, 2015. – 216 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:791193&theme=FEFU

2. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова – М. : Проспект, 2015. – 152 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:791159&theme=FEFU

3. В. Ф. Шаньгин Комплексная защита информации в корпоративных системах : учебное пособие для вузов. Москва : Форум, : Инфра-М, 2015. – 591 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:294516&theme=FEFU

4. В. В. Платонов Программно-аппаратные средства защиты информации : учебник для вузов / Москва : Академия, 2014. – 331 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:790443&theme=FEFU

5. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / М.А. Иванов, И.В. Чугунков. — Электрон. дан. — Москва : НИЯУ МИФИ, 2012. — 400 с. — Режим доступа: https://e.lanbook.com/book/75810

Дополнительная и справочная

(печатные и электронные издания)

1. Шаханова М.В. Современные технологии информационной безопасности : учебно-методический комплекс Москва : Проспект, 2015. – 216 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:791301&theme=FEFU

2. Метелица Н.Т. Вычислительные сети и защита информации [Электронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. текстовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 c. — Режим доступа: http://www.iprbookshop.ru/25962.html

3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : СПбГПУ, 2014. — 322 с. — Режим доступа: https://e.lanbook.com/book/64809

4. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] : учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: https://e.lanbook.com/book/5178

5. Васильков, А. В. Безопасность и управление доступом в информационных системах: учеб. пособие для сред. проф. образования / А. В. Васильков, И. А. Васильков. - М. : Форум, 2010. - 367 с. : ил., табл. - (Профессиональное образование). - Библиогр.: с. 356-358. — Режим доступа: http://znanium.com/bookread2.php?book=405313

6. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 c. — Режим доступа: http://www.iprbookshop.ru/43183.html.

7. Гатченко Н.А., Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации: учебник для вузов / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко; 4-е изд., перераб. и доп. - М.: Финансы и статистика, 2008. - 736с. — Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:355883&theme=FEFU

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Научная электронная библиотека eLIBRARY проект РФФИ www.elibrary.ru

2. Федеральный портал по научной и инновационной деятельности www.sci-innov.ru

3. Электронная библиотека НИЯУ МИФИ www.library.mephi.ru

4. Полнотекстовая база данных ГОСТов, действующих на территории РФ http://www.vniiki.ru/catalog/gost.aspx

5. Научная библиотека ДВФУ http://www.dvfu.ru/web/library/nb1

Перечень информационных технологий и программного обеспечения

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.	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) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18. Срок действия договора 20.09.2018. Лицензия до 30.06.2020. 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.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, 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) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18. Срок действия договора 20.09.2018. Лицензия до 30.06.2020. 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.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Комплексная безопасность вычислительных систем», составляет 18 часов.

На самостоятельную работу – 126 часа. При этом аудиторная нагрузка состоит из 8 лекционных часов и 10 часов практических занятий.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к практическим занятиям предполагает повторение лекционного материала. В результате обучающийся должен быть готов к выполнению заданий на практическом занятии. Основной практической составляющей является выполнение трех практических заданий с последующим предоставлением отчета о выполнении. По итогам выполнения задания проводится собеседование.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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 – 25). 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
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	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)

ИНЖЕНЕРНАЯ ШКОЛА

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Комплексная безопасность вычислительных систем»

Направление подготовки 09.06.01 Информатика и вычислительная техника

профиль «Вычислительные машины, комплексы и компьютерные сети»

Форма подготовки очная

Владивосток
2020

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-6 неделя обучения	Подготовка практического задания (выполнение отчета к занятию 1)	36	Отчет о выполнении практического задания
2	7-12 неделя обучения	Подготовка практического задания (выполнение отчета к занятию 2)	36	Отчет о выполнении практического задания
3	13-18 неделя обучения	Подготовка практического задания (выполнение отчета к занятию 3)	36	Отчет о выполнении практического задания
4	Сессия	Подготовка к зачету	18	Экзамен

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 1

Целью практического занятия 1 является приобретение навыков решения задач обеспечения безопасности предприятия.

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.

Методические указания к выполнению отчета по занятию 2

Целью практического занятия 2 является приобретение навыков решение задач эффективного кодирования.

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.

Методические указания к выполнению отчета по занятию 3

Целью практического занятия 3 является приобретение навыков решения задач обеспечения безопасности операционных систем.

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)

ИНЖЕНЕРНАЯ ШКОЛА

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Комплексная безопасность вычислительных систем»
Направление подготовки 09.06.01 Информатика и вычислительная техника
профиль «Вычислительные машины, комплексы и компьютерные сети»
Форма подготовки очная

Владивосток
2020

Паспорт ФОС

Код и формулировка компетентности	Этапы формирования компетентности	
ОПК-8 – готовность к преподавательской деятельности по основным образовательным программам высшего образования	Знает	основные требования к организации преподавательской деятельности
	Умеет	оценивать текущее состояние и тенденции развития образовательных программ в области информационных исследований
	Владеет	способами и демонстрации умения представлять результаты исследований
ПК-1 – способность выполнять теоретический анализ и экспериментальные исследования функционирования вычислительных машин, комплексов и компьютерных сетей с целью улучшения характеристик их функциональности и комплексной безопасности	Знает	основные требования к организации теоретических и экспериментальных исследований компьютерной техники
	Умеет	осуществлять отбор и использовать оптимальные сочетания теоретических и экспериментальных исследований
	Владеет	методами теоретических исследований обеспечения функциональности и безопасности вычислительных систем
УК-4 – готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	Знает	методы и технологии научной коммуникации на государственном и иностранном языках
	Умеет	следовать основным нормам, принятым в научном общении на государственном и иностранном языках
	Владеет	различными методами, технологиями и типами коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках
УК-6 – способность планировать и решать задачи собственного профессионального и личностного развития	Знает	содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда
	Умеет	формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей
	Владеет	способами выявления и оценки индивидуально-личностных, профессионально-значимых качеств и путями достижения более высокого уровня их развития

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Базовые задачи и методы обеспечения безопасности	ОПК-8, ПК-1, УК-4, УК-6	знает	собеседование (ОУ-1)	1-5
			умеет	коллоквиум (ОУ-2)	1-5
			владеет	конспект (ПР-7)	1-5
2	Раздел II. Угрозы и вирусы	ОПК-8, ПК-1, УК-4, УК-6	знает	собеседование (ОУ-1)	6-10
			умеет	коллоквиум (ОУ-2)	6-10
			владеет	конспект (ПР-7), отчет о выполнении практического задания	6-10
3	Раздел III. Формализация задач обеспечения безопасности вычислительных систем	ОПК-8, ПК-1, УК-4, УК-6	знает	собеседование (ОУ-1)	11-21
			умеет	коллоквиум (ОУ-2)	11-21
			владеет	конспект (ПР-7), отчет о выполнении практического задания	11-21
4	Раздел IV. Защита операционных систем	ОПК-8, ПК-1, УК-4, УК-6	знает	собеседование (ОУ-1)	22-30
			умеет	коллоквиум (ОУ-2)	22-30
			владеет	конспект (ПР-7), отчет о выполнении практического задания	22-30

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ОПК-8 – готовность к преподавательской деятельности по основным образовательным программам высшего образования	знает (пороговый уровень)	основные требования к организации преподавательской деятельности	сформированные представления о требованиях к формированию и реализации теоретических и экспериментальных исследований	комплексное видение организации методов проведения преподавательской деятельности в их взаимосвязи
	умеет (продвинутый)	оценивать текущее состояние и тенденции развития образовательных программ в области информационных исследований	отбор и аргументированное использование задач и результатов исследований с учетом специфики направленности (профиля) подготовки	отбор и оценивание задач и результатов исследования с использованием логико-математической интерпретации
	владеет (высокий)	способами и демонстрации умения представлять результаты исследований	Уверенное владение основными навыками общения в ходе информационных исследований	Успешно и творчески применяет навыки и методики исследования
ПК-1 – способность выполнять теоретический анализ и экспериментальные исследования функционирования вычислительных машин, комплексов и компьютерных сетей с целью улучшения характеристик их функциональности и комплексной безопасности	знает (пороговый уровень)	основные требования к организации теоретических и экспериментальных исследований компьютерной техники	сформированные представления о требованиях к формированию и реализации теоретических и экспериментальных исследований	комплексное видение организации теоретических и экспериментальных исследований в их взаимосвязи
	умеет (продвинутый)	осуществлять отбор и использовать оптимальные сочетания теоретических и экспериментальных исследований	отбор и использование методов исследований с учетом специфики направленности (профиля) подготовки	отбор и использование методов исследования с использованием логико-математической интерпретации
	владеет (высокий)	методами теоретических исследований обеспечения функциональности и безопасности вычислительных систем	Уверенное владение основными навыками общения в ходе информационных исследований	Успешно и творчески применяет навыки и методики исследования
УК-4 – готовность использовать современные методы и технологии научной коммуникации на госу-	знает (пороговый уровень)	методы и технологии научной коммуникации на государственном и иностранном языках	сформированные, но содержащие отдельные пробелы знания методов и технологий научной коммуникации на государственном и иностранном языках Сформированные, но содержащие от-	сформированные и систематические знания методов и технологий научной коммуникации на государственном и иностранном языках Сформированные систематические знания стилистиче-

дарственном и иностранном языках			дельные пробелы знания основных стилистических особенностей представления результатов научной деятельности в устной и письменной форме на государственном и иностранном языках	ских особенностей представления результатов научной деятельности в устной и письменной форме на государственном и иностранном языках
	умеет (продвинутый)	следовать основным нормам, принятым в научном общении на государственном и иностранном языках	в целом успешное, но содержащее отдельные пробелы умение следовать основным нормам, принятым в научном общении на государственном и иностранном языках	успешное и систематическое умение следовать основным нормам, принятым в научном общении на государственном и иностранном языках
	владеет (высокий)	различными методами, технологиями и типами коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках	в целом успешное, но сопровождающееся отдельными ошибками применение навыков анализа научных текстов на государственном и иностранном языках	успешное и систематическое применение навыков анализа научных текстов на государственном и иностранном языках
УК-6 – способность планировать и решать задачи собственного профессионального и личностного развития	знает (пороговый уровень)	содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда	сформированные, но содержащие отдельные пробелы знания основных методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных	смформированные систематические знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных
	умеет (продвинутый)	формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей	сформированные, но содержащие отдельные пробелы знания основных методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных	смформированные систематические знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных
	владеет (высокий)	способами выявления и оценки инди-	сформированные, но содержащие от-	смформированные систематические

		видуально-личностных, профессионально-значимых качеств и путями достижения более высокого уровня их развития	дельные пробелы знания основных методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных	знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Текущая аттестация студентов

Проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Проводится в форме контрольных мероприятий: защиты практических работ, собеседования по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем. Объектами оценивания выступают:

- учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);
- степень усвоения теоретических знаний (опрос);
- уровень овладения практическими умениями и навыками по всем видам учебной работы (разноуровненвые задачи и задания);
- результаты самостоятельной работы (разноуровненвые задачи и задания).

Промежуточная аттестация студентов

Проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Предусматривает устный опрос в форме ответов на вопросы экзаменационных билетов. В качестве оценочного средства используются экзаменационные билеты.

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Международные стандарты информационного обмена.

2. Получение статистических знаний об атаках, которым подвергаются компьютерные системы.

3. Современные методы защиты информации

4. Основные технологии построения защищенных информационных систем.

5. Место информационной безопасности в национальной безопасности страны. Концепция информационной безопасности.

6. Понятие угрозы. Три вида возможных нарушений информационной системы.

7. Виды противников или «нарушителей». Информационная безопасность в условиях функционирования в России глобальных сетей.

8. Понятия о видах вирусов. Получение знаний о существующих "компьютерных вирусах". Классификация "компьютерных вирусов".

9. Основные правила защиты от "компьютерных вирусов". Обзор антивирусных программ.

10. Методика использования антивирусных программ. Восстановление пораженных "компьютерными вирусами" объектов.

11. Модели безопасности и их применение.

12. Дискреционная и мандатная модели политики безопасности.

13. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

14. Анализ способов нарушений информационной безопасности.

15. Использование защищенных компьютерных систем.

16. Традиционные и современные криптосистемы.

17. Методы шифрования данных.

18. Основные криптографические алгоритмы.

19. Абонентское и пакетное шифрование.

20. Взаимное подтверждение подлинности (аутентификация) абонентов и объектов сети.

21. Обеспечение целостности информации на основе электронной цифровой подписи.

22. Методы несанкционированного доступа к операционным системам (ОС).

23. Основные механизмы функционирования ОС.

24. Основные термины безопасности ОС. Разграничение доступа к ОС.

25. Основные механизмы защиты в ОС Linux

26. Пользователи и группы в Linux. Разделение доступа. Системы мандатной защиты.

27. SELinux. Защита ОС в сети. Сетевые экраны. IPTables.

28. Основные механизмы защиты в ОС Windows

29. Пользователи и группы в Windows. Разделение доступа. Брандмауэр Windows.

30. Защита ОС в сети. Защита в Active Directory.

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.

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-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины

Форма экзаменационного билета

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное

учреждение высшего образования

«Дальневосточный федеральный университет»

ИНЖЕНЕРНАЯ ШКОЛА

Экзамен по дисциплине

«Комплексная безопасность вычислительных систем»

по направлению подготовки 09.06.01 Информатика и вычислительная техника

профиль «Вычислительные машины, комплексы и компьютерные сети»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Понятие угрозы. Три вида возможных нарушений информационной системы.

2. Модели безопасности и их применение.

3. Методы несанкционированного доступа к операционным системам (ОС).

Руководитель ОПОП Ю.В. Добржинский

И.о. зав. кафедрой ИБ Ю.В. Добржинский