



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК


«СОГЛАСОВАНО»
Руководитель ОП
«Информационная безопасность»



(подпись) Варлатая С.К.
(Ф.И.О. рук. ОП)

« 5 » июля 2018 г.

«УТВЕРЖДАЮ»
Заведующий (ая) кафедрой
информационной безопасности



(подпись) Добржинский Ю.В.
(Ф.И.О. рук. ОП)

« 5 » июля 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (РПУД)

«Информационная безопасность автоматизированных систем»

Направление –10.03.01 «Информационная безопасность»

Профиль подготовки - «Комплексная защита объектов информатизации»

Форма подготовки – очная

курс 3,4 семестр 6,7

лекции 36 час.

практические занятия 18 час.

лабораторные работы 72 час.

в том числе с использованием МАО лек. _____ / пр. _____ / лаб. _____ час.

всего часов аудиторной нагрузки 108 час.

в том числе с использованием МАО _____ час.

самостоятельная работа 72 час.

в том числе на подготовку к экзамену 36 час.

контрольные работы (количество) учебным планом не предусмотрены

курсовая работа / курсовой проект учебным планом не предусмотрены

зачет 7 семестр

экзамен 6 семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

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

Заведующий (ая) кафедрой: Добржинский Ю.В., к.т.н., с.н.с.

Составитель (ли): Гордеев С.И., к.т.н., доцент

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « _____ » _____ 20 г. № _____

Заведующий кафедрой _____ Ю.В. Добржинский
(подпись) (и.о. фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « _____ » _____ 200 г. № _____

Заведующий кафедрой _____ Ю.В. Добржинский
(подпись) (и.о. фамилия)

Аннотация к рабочей программе дисциплины «Информационная безопасность автоматизированных систем»

Рабочая программа по курсу «Информационная безопасность автоматизированных систем» разработана для студентов по направлению 10.03.01 «Информационная безопасность».

Общая трудоемкость освоения дисциплины составляет 216 часов (6 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (72 час.), самостоятельная работа студентов (72 час.), контроль качества обучения студентов (36 час.). Дисциплина реализуется на 3, 4 курсе в 6, 7 семестре. Форма контроля по дисциплине – экзамен в 6 семестре, зачет в 7 семестре.

Цель дисциплины - раскрыть содержание основных понятий, методов и механизмов обеспечения информационной безопасности автоматизированных систем.

Задачи дисциплины – дать основы:

- системного и комплексного подхода к анализу и обеспечению информационной безопасности АС в процессах их создания и эксплуатации (администрирования);
- представления, анализа и обоснования моделей, методов и механизмов обеспечения информационной безопасности АС;
- практических навыков работы с нормативно-методическими документами(стандартами) в сфере информационной безопасности автоматизированных информационных систем.

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

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-2) способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	программные средства системного, прикладного и специального назначения для защиты информации, а так же современные инструментальные средства, языки и системы программирования
	Умеет	применять для различных целей программные средства системного, прикладного и специального назначения
	Владеет	современными и широко используемыми языками и системами программирования для решения профессиональных задач
(ПК-8) способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знает	принципы и методы проектирования подсистем и средств обеспечения информационной безопасности
	Умеет	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности систем
	Владеет	методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов и технико-экономической экспертизы
(ПК-9) способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знает	основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет	пользоваться нормативными и техническими документами по защите информации
	Владеет	навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию
(ПК-16) способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять	Знает	ролевую политику и технологии индивидуально-группового доступа к разделяемым информационным ресурсам;
	Умеет	вырабатывать перечень процедур и работ по администрированию защищенных АС.
	Владеет	навыками работы с нормативно-методическими документами в сфере информационной безопасности

процессом их реализации		автоматизированных информационных систем.
-------------------------	--	---

Для формирования вышеуказанных компетенций в рамках дисциплины «Информационная безопасность автоматизированных 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), лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

РАЗДЕЛ 1. ИНФОРМАЦИЯ КАК ОБЪЕКТ ЗАЩИТЫ (18 часов)

Тема 1. Защита человека от опасной информации и от не информированности (6 часа)

Понятие угрозы, виды и классификация угроз. Информация, представляющая угрозу для общества и государства. Конституционное право гражданина на получение информации. Понятие «Информационный голод».

Тема 2. Свойства информации как объекта защиты на различных уровнях ее представления (6 часа)

Информационный шум. Понятия «информация», «сообщение», «сигнал», «носитель». Их связь между собой. Семантическая и признаковая информация. Их классификация. Понятие «Защита информации». Компьютерная информация и особенности ее защиты. Кодирование информации, защитные функции. Семантический и прагматический уровни защиты информации.

Тема 3. Информация как ценность. Понятие об информационных угрозах (6 часа)

Понятия ценности и стоимости информации. Соотношение ценности информации с ее прагматическими свойствами. Угрозы конфиденциальности. Понятие, виды, задачи. Стратегия управление риском.

РАЗДЕЛ 2. АНАЛИЗ ИСТОРИЧЕСКИ СЛОЖИВШИХСЯ НАПРАВЛЕНИЙ ИНФОРМАЦИОННОЙ ЗАЩИТЫ (18 часов)

Тема 1. Нормативно-правовое регулирование защиты информации (2 час)

Законодательные меры для защиты от опасной информации. Противодействие неинформативности граждан. Секретные сведения. Государственная тайна. Коммерческая тайна. Профессиональная тайна. Лицензирование услуг по защите информации. Недостатки, свойственные нормативно-правовой защите информационных отношений.

Тема 2. Организационно-распорядительная защита (2 час)

Понятие организационно-распорядительной защиты. Регламент работы с конфиденциальной информацией. Контроль за персоналом, его формы. Администратор безопасности.

Тема 3. Инженерная защита и техническая охрана объектов информатизации (2 час)

Понятие инженерной защиты объектов информатизации; цели и задачи. Построение технической охраны объектов информатизации.

Тема 4. Защита информации от утечки по техническим каналам (2 час)

Термин «утечка информации по техническому каналу». Понятие и виды каналов утечки информации.

Тема 5. Обнаружение и нейтрализация средств технической разведки (2 час)

Классификация средств технической разведки. Способы обнаружения средств технической разведки. Способы нейтрализации средств технической разведки.

Тема 6. Управление доступом к информации (2 час)

Система управления доступом. Аутентификация, виды и особенности. Разграничение прав доступа к объектам.

Тема 7. Защита компьютерной информации и компьютерных систем от вредоносных программ (2 час)

Понятие «вредоносное программное воздействие». Признаки вредоносных программ. Компьютерные вирусы, мифические вирусы. Программные закладки. Обеспечение безопасности АС.

Тема 8. Семантическое сокрытие информации (2 час)

Термин «семантическое сокрытие информации». Виды криптосистем, их особенности.

Тема 9. Обеспечение нормальных условий эксплуатации автоматизированных информационных систем (АИС) и машинных носителей информации (2 час)

Методы обеспечения нормальных условий эксплуатации АИС и носителей информации. Виды дестабилизирующих воздействий и способы борьбы с ними. Составляющие технической эксплуатации АИС. Основные меры по защите АИС.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (18 часов)

Практическая работа № 1. Выявление и анализ угроз безопасности информации в документообороте предприятия (4.5 час.)

Цель:

1. Получить практические навыки в выявлении угроз безопасности информации
2. Закрепить навыки анализа рисков безопасности
3. Закрепить знания, полученные на лекциях

Практическая работа № 2. Подбор технических средств для обеспечения защиты информации (4.5 час.)

Цель:

1. Закрепить знания, полученные на лекциях.

2. Получить практические навыки в решении многокритериальных задач.
3. Получить опыт исследования слабо формализуемых проблем и методов их решения.

Практическая работа № 3. Анализ рисков безопасности информации (4.5 час.)

Цель:

1. Получить навыки оценки рисков безопасности информационной системы предприятия.
2. Получить практический опыт подбора критериев информационной безопасности системы
3. Закрепить теоретические навыки, полученные на лекциях

Практическая работа № 4. Проверка защищенности объекта на соответствие нормативным документам (4.5 час.)

Цель: проверить защищенность объекта.

Лабораторные работы (72 час.)

1. Удостоверяющие центры на основе службы сертификации в операционной системе Windows 2003 Server (18 часов)
2. Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя. (18 часов)
3. Генерация ключевой информации и криптографические средства в клиентской программе электронной почты (18 часов)
4. Защита программ от несанкционированного использования с помощью USB-ключей и средств разработчика (18 часов)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Информационная безопасность автоматизированных 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.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	РАЗДЕЛ 1. ИНФОРМАЦИЯ КАК ОБЪЕКТ ЗАЩИТЫ	ОПК-5 ПК-2, ПК-8, ПК-9, ПК-16	знает	ПР-1	1-11
			умеет	ПР-6	1-11
			владеет	ПР-7	1-11
2	РАЗДЕЛ 2. АНАЛИЗ ИСТОРИЧЕСКИ СЛОЖИВШИХСЯ НАПРАВЛЕНИЙ ИНФОРМАЦИОННОЙ ЗАЩИТЫ	ОПК-5 ПК-2, ПК-8, ПК-9, ПК-16	знает	ПР-1	12-25
			умеет	ПР-6	12-25
			владеет	ПР-7	12-25

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. — (Среднее профессиональное образование). - Режим доступа: <http://znanium.com/catalog/product/915902>
2. Петров, С. В. Информационная безопасность [Электронный ресурс] : учебное пособие / С. В. Петров, П. А. Кисляков. — Электрон. текстовые данные. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: <http://www.iprbookshop.ru/33857.html>
3. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/546679>

Дополнительная литература

(печатные и электронные издания)

1. Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева. — Москва : Русайнс, 2016. — 354 с. — Для бакалавров. — ISBN 978-5-4365-0960-0. <http://lib.dvfu.ru:8080/lib/item?id=BookRu:BookRu-920736&theme=FEFU>
2. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М. : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — <https://doi.org/10.12737/4868>. - Режим доступа: <http://znanium.com/catalog/product/937469>
3. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2006. - 543 с <http://lib.dvfu.ru:8080/lib/item?id=chamo:350791&theme=FEFU>

Интернет - источники

1. http://e.lanbook.com/books/element.php?p11_cid=25&p11_id=682 - О.К. Скляров «Волоконно-оптические сети и системы связи», Издательство: "Лань", Год: 2010, Издание: 2-е, стер., Объем: 272 стр.

2. <http://padabum.com/d.php?id=2562> - В. Олифер, Н. Олифер
 “Компьютерные сети. Принципы, технологии, протоколы” СПб.: Питер,
 2010, 944 с.

3. Алиев Т.И. Сети ЭВМ и телекоммуникации [Электронный ресурс]/
 Алиев Т.И.— Электрон. текстовые данные.— СПб.: Университет ИТМО,
 2011.— 400 с.— <http://www.iprbookshop.ru/68120.html>

Перечень информационных технологий и программного обеспечения

<p>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.</p>	<p>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 University 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 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019</p>
<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 741, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего</p>	<p>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 University 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.</p>

<p>контроля промежуточной аттестации.</p>	<p>и Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. б) 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</p>
---	--

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Информационная безопасность автоматизированных систем», составляет 126 часов. На самостоятельную работу – 54 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов, 18 часов практических занятий и 72 часов лабораторных работ.

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

Подготовка к практическим занятиям и лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и лабораторных работ. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении.

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, материалов по практическим занятиям и лабораторным работам.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

<p>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.</p>	<p>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 видеочамера Multipix MP-HD718 Доска аудиторная</p>
<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 741, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 50) Оборудование: "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 видеочамера Multipix MP-HD718" Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.</p>



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

**УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ
РАБОТЫ ОБУЧАЮЩИХСЯ**

**по дисциплине «Информационная безопасность автоматизированных
систем»**

**Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»**

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 практических заданий и лабораторных работ.	27	Отчет о выполнении
2	Сессия	Подготовка к экзамену	27	Экзамен

Подготовка отчетов к практическим заданиям и лабораторным работам предполагает повторение лекционного материала и выполнение практических заданий и лабораторных работ. В результате студент должен представить отчеты о проделанной работе.

Методические рекомендации к работе с литературными

источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.
4. Текущее тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентами учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности,

варианты действий;

- умение сформировать свою позицию, оценку и аргументировать ее.

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	Оценка
От 95% до 100%	отлично
От 76% до 95%	хорошо
От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по практическим занятиям и лабораторным работам.



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Информационная безопасность автоматизированных
систем»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции	
способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);	Знает	Программные средства системного, прикладного и специального назначения для защиты информации, а так же современные инструментальные средства, языки и системы программирования
	Умеет	Применять для различных целей программные средства системного, прикладного и специального назначения
	Владеет	Современными и широко используемыми языками и системами программирования для решения профессиональных задач
способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-8)	Знает	Принципы и методы проектирования подсистем и средств обеспечения информационной безопасности
	Умеет	Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности систем
	Владеет	Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов и технико-экономической экспертизы
способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-9).	Знает	Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет	Пользоваться нормативными и техническими документами по защите информации
	Владеет	Навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию
способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по	Знает	Ролевую политику и технологии индивидуально-группового доступа к разделяемым информационным ресурсам;
	Умеет	Вырабатывать перечень процедур и работ по администрированию защищенных АС.

обеспечению информационной безопасности, управлять процессом их реализации (ПК-16)	Владеет	Навыками работы с нормативно-методическими документами в сфере информационной безопасности автоматизированных информационных систем.
способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);	Знает	Источники изъятий безопасности, основы активного аудита безопасности в распределенных АС;
	Умеет	Анализировать и определять функциональные требования безопасности по классам защищенности АС;
	Владеет	Навыками работы с нормативно-методическими документами в сфере информационной безопасности автоматизированных информационных систем.

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства - наименование		
			текущий контроль	промежуточная аттестация	
1	РАЗДЕЛ 1. ИНФОРМАЦИЯ КАК ОБЪЕКТ ЗАЩИТЫ	ОПК-16 ПК-2, ПК-8, ПК-9, ПК-16	знает	ПР-1	1-11
			умеет	ПР-6	1-11
			владеет	ПР-7	1-11
2	РАЗДЕЛ 2. АНАЛИЗ ИСТОРИЧЕСКИ СЛОЖИВШИХСЯ НАПРАВЛЕНИЙ ИНФОРМАЦИОННОЙ ЗАЩИТЫ	ОПК-16 ПК-2, ПК-8, ПК-9, ПК-16	знает	ПР-1	12-25
			умеет	ПР-6	12-25
			владеет	ПР-7	12-25

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Понятие, виды и структура автоматизированных информационных систем

2. Функции и структура АС
3. Безопасность АС, ее составляющие
4. Субъекты и объекты обеспечения информационной безопасности
в АС
5. Принципы, основные методы и механизмы обеспечения
безопасности информации в АС
6. Классификация, идентификация и спецификация угроз
безопасности в АС
7. Скрытые каналы утечки информации в АС
8. Целостность данных
9. Общая характеристика, виды и архитектура документальных АС
10. Общие положения по эксплуатации АС
11. Особенности эксплуатации и администрирования защищенных
АИС.
12. Политика, модели и механизмы дискреционного разграничения
доступа
13. Политика, модели и механизмы мандатного разграничения
доступа
14. Политика и модели ролевого доступа
15. Технологии индивидуально-группового доступа
16. Понятие разграничения доступа
17. Виды и программно-техническая структура распределенных АС
18. Особенности политики и систем безопасности в распределенных
АС
19. Уязвимости систем защиты, системы активного аудита
безопасности в распределенных АС
20. Дискреционная модель обеспечения целостности данных Кларка-
Вильсона
21. Мандатная модель обеспечения целостности даны Кена Биба
22. Объединение мандатных моделей Белла-ЛаПадуллы и Кена Биба

23. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС
24. Показатели защищенности, классификация АС по требованиям защиты от НСД к информации
25. Критерии оценки безопасности информационных технологий



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по дисциплине «Информационная безопасность автоматизированных
систем»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

Владивосток
2019

Количество аудиторных часов, отведенных на изучение дисциплины «Информационная безопасность автоматизированных систем», составляет 126 часов. На самостоятельную работу – 54 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов, 18 часов практических занятий и 72 часов лабораторных работ.

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

Подготовка к практическим занятиям и лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и лабораторных работ. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении.

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, материалов по практическим занятиям и лабораторным работам