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

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

«СОГЛАСОВАНО»
Руководитель ОП

Бережнова Е.И.,
(подпись) (Ф.И.О. рук. ОП)
«29» июня 2018 г.

«УТВЕРЖДАЮ»
Заведующий (ая) кафедрой
информационной безопасности

Добржинский Ю.В.
(подпись) (Ф.И.О. зав. каф.)
«28» июня 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Специальность: 38.05.01 Экономическая безопасность
Специализация: «Экономико-правовое обеспечение экономической безопасности».
Форма подготовки очная

курс _4_ семестр _8_
лекции _18_ час.
практические занятия _18_ час.
практические работы _-_ час.
в том числе с использованием МАО лек. _-_ / пр. _18 / лаб. _-_ час.
всего часов аудиторной нагрузки _36_ час.
в том числе с использованием МАО _18_ час.
самостоятельная работа _72_ час.
в том числе на подготовку к зачету _-_ час.
контрольные работы (количество) _-_
курсовая работа / курсовой проект _-_семестр
зачет _8 семестр
зачет _не предусмотрен

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от _16.01.2017 № _20_

Рабочая программа обсуждена на заседании кафедры информационной безопасности, протокол № _6_ от 28 июня__ __ 2018 г.

Заведующий кафедрой: д-р экон. наук, проф. Добржинский Ю.В.
Составители: старший преподаватель В.В. Ерофеев

Владивосток
2018

.

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 201 г. № _____

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

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 201 г. № _____

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

.

Аннотация

к рабочей программе дисциплины

«Защита информации»

Учебный курс «Защита информации» (On-line course) предназначен для студентов специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правое обеспечение экономической безопасности» и «Экономика и организация производства на режимных объектах».

Общая трудоемкость дисциплины 4 зачетные единицы, 144 часа. Учебным планом предусмотрены практические занятия (8 часов), самостоятельная работа (136 часов) в рамках дистанционного курса. Дисциплина реализуется на 3 курсе в 5 семестре.

Дисциплина «Защита информации» входит в блок обязательных дисциплин базовой части «Дисциплины (модули)» учебного плана. Дисциплина «Защита информации» является онлайновой.

Курс «Защита информации» введен с целью развития у обучающихся в учреждениях высшего образования профессиональных навыков в области защиты информации в рамках направления «Экономическая безопасность». Актуальность предмета обусловлена растущими технологическими возможностями современных информационных систем, которые играют ключевую роль в развитии хозяйственно-экономических отношений, политических и нормативно-правовых. В настоящее время информационная безопасность является приоритетным сегментом в работе крупных предприятий, государственных органов и страны в целом.

Содержание дисциплины охватывает следующий круг вопросов. Концепция защиты информации. Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Угрозы конфиденциальной информации. Правовая защита. Организационная защита. Инженерно-техническая защита. Физические средства защиты. Охранные системы. Зоны безопасности. Охранное телевидение. Системы контроля доступа. Системы опознавания по отпечаткам пальцев. Си-

стемы опознавания по голосу. Система опознавания по геометрии рук. Аппаратные средства защиты. Программные средства защиты. Защита информации от несанкционированного доступа. Защита от копирования. Защита информации от разрушения. Криптографические средства защиты. Технология шифрования речи. Информационная защита персонального компьютера (ПК). Основы защиты ПК: логика и приемы. Предотвращение потери данных при аварии. Внесистемные рабочие диски и хранилища. Временная блокировка системы Просмотр "следов" в файлах. Удаление пунктов меню. Редактирование/Переименование пунктов меню. Системы защиты паролем Windows. Качественное программное обеспечение для защиты паролем. Условно бесплатные программы. Коммерческое программное обеспечение. Программное обеспечение для шифрования Magic Folder (EMF) Secret Stuff Good Privacy (PGP). Безопасность и конфиденциальность в Internet. Интернет и компьютерный взлом. Средства защиты электронной почты. Вирусы и антивирусная защита. Шифр «Сцитала». Шифр Цезаря. Предмет криптографии. "Исторические" шифры и криптографические алгоритмы. Электронные цифровые подписи. Технология создания и использования электронной цифровой подписи (ЭЦП) на асимметричных криптосистемах. Закон об электронной цифровой подписи.

Для успешного изучения дисциплины «Защита информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач;

способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, применять в профессиональной деятельности автоматизированные информационные системы, используемые в экономике, автоматизированные рабочие места, проводить информационно-поисковую

работу с последующим использованием данных при решении профессиональных задач;

способность на основе статистических данных исследовать социально-экономические процессы в целях прогнозирования возможных угроз экономической безопасности.

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОК-8 - способность принимать оптимальные организационно-управленческие решения	Знает	Основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации для принятия оптимальных организационно-управленческих решений
	Умеет	Применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
	Владеет	Навыками работы с различными информационными ресурсами и технологиями
ПК-1 - способность подготавливать исходные данные, необходимые для расчета экономических показателей, характеризующих деятельность хозяйствующих субъектов	Знает	Методы подготовки исходных данных, необходимых для расчета экономических показателей, характеризующих деятельность хозяйствующих субъектов
	Умеет	Собирать и анализировать исходные данные для расчетов, прогнозировать угрозы информационной безопасности
	Владеет	Инструментами исследования и обобщения причин и последствий, выявленных в результате контроля отклонений, нарушений и недостатков
ПСК-1 - способность исследовать и обобщать причины и последствия, выявленные в результате контроля отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение	Знает	Методы контроля отклонений, нарушений и недостатков и приемы подготовки предложений, направленных на их устранение
	Умеет	Собирать и анализировать исходные данные для расчетов, прогнозировать угрозы информационной безопасности
	Владеет	Инструментами исследования и обобщения причин, выявленных в результате контроля отклонений, нарушений и недостатков

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ (8 час)

.

Тема 1. Понятие информационной безопасности. Основные составляющие информационной безопасности (2 часа)

Информационная безопасность, защита информации. Конфиденциальность, целостность, доступность информации.

Тема 2. Угрозы информационной безопасности АС (6 часа)

Основные определения и критерии классификации угроз. Источник угрозы, атака. Непреднамеренные ошибки пользователей. Вредоносное программное обеспечение. Перехват данных.

Раздел 2. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (4 часов)

Тема 1. Законодательный уровень информационной безопасности (2 часа)

Закон "Об информации, информатизации и защите информации", Закон о защите персональных данных.

Тема 2. Понятие стандарта в области информационной безопасности (2 часа)

Основные понятия. Механизмы безопасности. Классы безопасности.

Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (6 час)

Тема 1. Управление рисками (2 часа)

Управление рисками. Подготовительные этапы. Идентификация рисков.

Тема 2. Уровни информационной безопасности (2 часа)

Классы мер: управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ. Идентификация и аутентификация. Протоколирование и аудит, шифрование, контроль целостности

.

Тема 3. Особенности современных информационных систем, существенные с точки зрения безопасности (2 часа)

Архитектура клиент-сервер, внешние сервисы, облачные платформы Microsoft Azure, Amazon EC2. SIEM системы.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические работы (36 час., в том числе МАО – 18 час.)

Практическая работа №1. Технологии организации и защиты данных (8 ч.)

Практическая работа №2. Методы выявления угроз безопасности (8 ч.) (*Метод активного обучения - мастер-класс*)

Практическая работа №3. Средства мониторинга ИТ инфраструктуры предприятия (4 ч.) (*Метод активного обучения - мастер-класс*)

Практическая работа №4. Мероприятия по обеспечению информационной безопасности (8 ч.) (*Метод активного обучения - разработка индивидуального проекта)*

Практическая работа №5. Технологии построения информационных систем с точки зрения информационной безопасности. (4 ч.) (*Метод активного обучения - разработка индивидуального проекта)*

Практическая работа №6. Облачные технологии, сервисы и вычисления (4 ч.) (*Метод активного обучения - разработка индивидуального проекта)*

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Защита информации» 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;

.

- характеристику заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

- требования к представлению и оформлению результатов самостоятельной работы;

- критерии оценки выполнения самостоятельной работ.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ, ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ Тема 1, 2 Раздел 2. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (8 часов) Тема 1, 2	ОК-12	Основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	конспект (ПР-7); практическая работа (ПР-6)	Вопросы к зачету 1, 4
			Применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	практическая работа (ПР-6)	Вопросы к зачету 1, 4
			Навыками работы с различными информационными ресурсами и технологиями	практическая работа (ПР-6); контрольная работа (ПР-2)	Вопросы к зачету 1, 4
2	Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Тема 1, 2	ПСК-1	Методы контроля отклонений, нарушений и недостатков и Приемы подготовки предложений, направленных на их устранение	конспект (ПР-7); практическая работа (ПР-6)	Вопросы к зачету 2,3,5,6,7,8
			Собирать и анализировать исходные данные для расчетов, прогнозировать угрозы информационной безопасности	практическая работа (ПР-6)	Вопросы к зачету 2,3,5,6,7,8
			Инструментами исследования и обобщения причин и последствий выявленных в результате контроля отклонений, нарушений и недостатков	практическая работа (ПР-6); контрольная работа (ПР-2); деловая игра (ПР-10)	Вопросы к зачету 2,3,5,6,7,8

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. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-627-0 – http://znanium.com/catalog/product/420047
2. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с http://www.iprbookshop.ru/6991.html
3. Анализ состояния защиты данных в информационных системах [Электронный ресурс]: учебно-методическое пособие/ — Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2012.— 52 с http://www.iprbookshop.ru/44897.html
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные. — Саратов: Профобразование, 2017.— 702 с. http://www.iprbookshop.ru/63594.html
5. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика»/ Фомин Д.В. — Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 125 с. http://www.iprbookshop.ru/77318.html

Дополнительная литература

(печатные и электронные издания)

.

1.Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60x88 1/16 + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3 http://znanium.com/catalog/product/549914

2. Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 186 с http://www.iprbookshop.ru/7008.html

3.Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5 http://znanium.com/catalog/product/997108

4. Горюхина Е.Ю. Информационная безопасность [Электронный ресурс]: учебное пособие/ Горюхина Е.Ю., Литвинова Л.И., Ткачева Н.В.— Электрон. текстовые данные.— Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015.— 221 с http://www.iprbookshop.ru/72672.html

5. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Обложка. КБС) ISBN 978-5-00091-007-8 http://znanium.com/catalog/product/544554

6. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - http://znanium.com/catalog/product/763644

.

7. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. https://e.lanbook.com/book/39990
8. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: -: http://znanium.com/catalog/product/987215

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Электронная библиотека и базы данных ДВФУ. http://dvfu.ru/web/library/elib
2. Электронно-библиотечная система «Лань» http://e.lanbook.com
3. Электронно-библиотечная система «Научно-издательского центра ИНФРА-М» http://znanium.com
4. Электронно-библиотечная система БиблиоТех. http://www.bibliotech.ru
5. Электронный каталог научной библиотеки ДВФУ http://lib.dvfu.ru:8080/search/query?theme=FEFU
6. Научная библиотека КиберЛенинка: http://cyberleninka.ru/

Перечень информационных технологий и программного обеспечения

Перечень информационных технологий и программного обеспечения дисциплины «Защита информации» включает следующее:

Программное обеспечение:

1. Программные средства: Приложения к MS Windows, MS Office, Kerio Control, Kaspersky Endpoint Security, средство мониторинга WireShark, case-средства:, MS Visio, облачная платформа Microsoft Azure

Бесплатные программные средства для управления проектами.

.

2. Программное приложение Microsoft Office Power Point (для чтения лекционного материала и представления презентационных докладов на практических занятиях).

Информационные технологии:

– сбор, хранение, систематизация и выдача учебной и научной информации;

– обработка текстовой, графической и эмпирической информации;

– подготовка, конструирование и презентация итогов исследовательской и аналитической деятельности;

– самостоятельный поиск дополнительного учебного и научного материала, с использованием поисковых систем и сайтов сети Интернет, электронных энциклопедий и баз данных;

– использование электронной почты преподавателей и обучающихся для рассылки, переписки и обсуждения возникших учебных проблем.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Реализация дисциплины «Защита информации» предусматривает следующие виды учебной работы: лекции, практические работы, самостоятельную работу студентов, текущий контроль и промежуточную аттестацию.

Освоение курса дисциплины «Защита информации» предполагает рейтинговую систему оценки знаний студентов и предусматривает со стороны преподавателя текущий контроль за посещением студентами лекций, подготовкой и выполнением всех лабораторных работ с обязательным предоставлением отчета о работе, выполнением всех видов самостоятельной работы.

Промежуточной аттестацией по дисциплине «Защита информации» является зачет, который проводится в виде тестирования.

В течение учебного семестра обучающимся нужно:

- освоить теоретический материал (20 баллов);
- успешно выполнить аудиторные и контрольные задания (50 баллов);

.

• своевременно и успешно выполнить все виды самостоятельной работы (30 баллов).

Студент считается аттестованным по дисциплине «Защита информации» при условии выполнения всех видов текущего контроля и самостоятельной работы, предусмотренных учебной программой.

Критерии оценки по дисциплине «Защита информации» для аттестации на зачете следующие: 86-100 баллов – «отлично», 76-85 баллов – «хорошо», 61-75 баллов – «удовлетворительно», 60 и менее баллов – «неудовлетворительно».

Пересчет баллов по текущему контролю и самостоятельной работе производится по формуле:

$$P(n) = \sum_{i=1}^{m} \left[\frac{O_i}{O_i^{max}} \times \frac{k_i}{W} \right],$$

где: $W = \sum_{i=1}^{n} k_i^n$ для текущего рейтинга;

$W = \sum_{i=1}^{m} k_i^n$ для итогового рейтинга;

P(n) – рейтинг студента;

m – общее количество контрольных мероприятий;

n – количество проведенных контрольных мероприятий;

O_i – балл, полученный студентом на *i*-ом контрольном мероприятии;

O_i^{max} – максимально возможный балл студента по *i*-му контрольному мероприятию;

k_i – весовой коэффициент *i*-го контрольного мероприятия;

k_i^n – весовой коэффициент *i*-го контрольного мероприятия, если оно является основным, или 0, если оно является дополнительным.

Рекомендации по планированию и организации времени, отведенного на изучение дисциплины

Оптимальным вариантом планирования и организации студентом време-

ни, необходимого для изучения дисциплины, является равномерное распределение учебной нагрузки, т.е. систематическое ознакомление с теоретическим материалом на лекционных занятиях и закрепление полученных знаний при подготовке и выполнении лабораторных работ и заданий, предусмотренных для самостоятельной работы студентов.

Подготовку к выполнению лабораторных работ необходимо проводить заранее, чтобы была возможность проконсультироваться с преподавателем по возникающим вопросам. В случае пропуска занятия, необходимо предоставить письменную разработку пропущенной практической работы.

Самостоятельную работу следует выполнять согласно графику и требованиям, предложенным преподавателем

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для осуществления образовательного процесса необходимо следующее техническое обеспечение – это аудитория с мультимедийным оборудованием с доступом в сеть «Интернет».

Комплект презентационного оборудования: проектор, экран (для представления лекционного материала и презентации докладов на практическом занятии, а также для представления результатов самостоятельной и научно-исследовательской работы).

В читальных залах Научной библиотеки ДВФУ предусмотрены рабочие места для людей с ограниченными возможностями здоровья, оснащены дисплеями и принтерами Брайля; оборудованные портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами, видеоувеличителем с возможностью регуляции цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками.

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья ДВФУ все здания оборудованы

.

пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной системы.

Приложение 1

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

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине Защита информации
«Специальность: 38.05.01 Экономическая безопасность
Специализация: «Экономико-правовое обеспечение экономической безопасности».
Форма подготовки очная

Владивосток
2018

.

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	Еженедельно в течение семестра	Подготовка к лекциям, изучение конспектов лекций;	(1,5 час. в неделю) 27 часов	Опрос Собеседование
2	В течение семестра	Подготовка к практическим работам	(2 час. в неделю) 36 часов	Сдача работы
3	В течение семестра	Подготовка к зачету	9 часов	Собеседование
		итого	72 часов	

Мметодические рекомендации при работе над конспектом лекций

В ходе лекционных занятий необходимо вести конспектирование учебного материала. При этом необходимо обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале.

Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной и дополнительной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

При подготовке к лекции необходимо ознакомится с вопросами темы

лекции, представленными в рабочей учебной программе. Выписать все определения основных понятий темы. Без знания определений сложно усвоить экономические законы, закономерности, функциональные зависимости и другие вопросы. Целесообразно иметь у себя какой-либо экономический словарь. После уяснения сути ключевых понятий необходимо повторить те вопросы, которые были изложены преподавателем на предшествующей лекции.

После изучения материалов лекций следует обратиться к рекомендованной литературе для ответа на вопросы, выносимые на самостоятельное изучение, сделать необходимые выписки. Старайтесь сразу же приводить собственные примеры, связывать материал с известными сведениями, практикой, личным опытом. После этого можно переходить к выполнению тестов и решению задач Целесообразно делать себе поясняющие пометки, так как при проверке данных заданий преподаватель может попросить пояснить ваш выбор варианта ответа в тесте или ход решения задачи.

Методические рекомендации по подготовке к лабораторным работам

Критериями подготовленности студентов к лабораторным работам считается знания соответствующей литературы, владение методами исследования, выделение сущности явления в изучаемом материале, способность иллюстрировать существующие положения самостоятельно подобранными примерами.

При выполнении практической работы по дисциплине «Защита информации» необходимо изучить литературу, указанную в конце работы. Начинается работа с указания целей, к достижению которых студент должен стремиться.

Непосредственно задания состоят из нескольких разделов. В заданиях нет подробных инструкций к их выполнению, т.е. студент должен самостоятельно выбрать способы выполнения работы, воспользовавшись

конспектами лекций и той литературой, которая приведена в работе.

Отчет выполняется в электронном виде, снабжается описанием выполнения заданий и необходимыми диаграммами, которые представлены скриншотами моделей, выполненных с помощью необходимых программных средств. В отчете студент должен указать используемое программное средство и объяснить причину его использования. Отчет принимается преподавателем в форме собеседования, при этом студент должен отвечать на контрольные вопросы, приведенные в работе. Если будут выполнены все задания, и получены ответы на поставленные работы, только в этом случае работа считается сданной.

Методические рекомендации по подготовке к зачету

Зачет – это заключительный этап изучения дисциплины «Защита информации», имеющий целью проверить теоретические знания студента, его навыки и умение применять полученные знания при решении практических задач. Зачет проводится в объеме учебной программы по дисциплине в устной форме.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором студенты получают общую установку преподавателя и перечень основных требований к текущей и промежуточной аттестации. При этом важно с самого начала планомерно осваивать материал, руководствуясь, прежде всего перечнем вопросов по лекционным и практическим занятиям, конспектировать важные для решения учебных задач источники. В течение семестра происходят пополнение, систематизация и корректировка студенческих наработок, освоение нового и закрепление уже изученного материала.

Дисциплина «Защита информации» разбита на разделы, которые представляют собой логически завершенные части рабочей программы курса и являются тем комплексом знаний и умений, которые подлежат контролю.

Лекции и практические работы являются важными этапами подготовки к зачету, поскольку позволяют студенту оценить уровень собственных

знаний и своевременно восполнить имеющиеся пробелы.

Успешное освоение материала дисциплины требует от студента систематической работы:

- не пропускать аудиторные занятия (лекции, практические работы);
- своевременно выполнять практические работы;
- регулярно систематизировать материал записей лекционных, практических занятий: написание содержания занятий с указанием страниц, выделением (подчеркиванием, цветовым оформлением) тем занятий, составление своих схем, таблиц.

Систематическая и своевременная работа по освоению материалов по дисциплине «Защита информации» становится залогом получения высокой оценки знаний (в соответствии с рейтинговой системой оценок).

Таким образом, зачет выставляется без опроса – по результатам работы студента в течение семестра. Для этого студенту необходимо посетить все лекционные и практические занятия, активно работать на них, устно доказать знание основных понятий и терминов по дисциплине «Защита информации».

Студенты, не прошедшие по рейтингу, готовятся к зачету согласно вопросам к зачету, на котором должны показать, что материал курса ими освоен. При подготовке к зачету студенту необходимо:

– ознакомиться с предложенным списком вопросов;

– повторить теоретический материал дисциплины, используя материал лекций, практических занятий, учебников, учебных пособий;

– повторить основные понятия и термины;

– ответить на вопросы теста (фонд тестовых заданий).

Для получения зачета по дисциплине «Защита информации» предлагается два задания в виде вопросов, носящих теоретический. Время на подготовку к зачету устанавливается в соответствии с общими требованиями, принятыми в ДВФУ.

.

Неудовлетворительный ответ, демонстрирующий незнание понятийного аппарата (терминов, понятий), непонимание, незнание теоретического материала, систематическое непосещение занятий, является основанием для выставления оценки «неудовлетворительно» и не сдачи зачета.

Пересдача неудовлетворительного результата назначается в соответствии с общими требованиями, принятыми в ДВФУ.

Методические рекомендации по выполнению самостоятельной работы

Под самостоятельной работой студента понимается вид учебно-познавательной деятельности по освоению основной образовательной программы высшего образования, осуществляемой в определенной системе, при партнерском участии преподавателя в ее планировании и оценке достижения конкретного результата.

Цель данного вида работы студента – закрепить знания, умения и навыки, полученные в ходе аудиторных занятий (лекций, практических занятий). Это актуализирует процесс образования и наполняет его осознанным стремлением к профессионализму. Данный вид работы осуществляется под руководством преподавателя, который выполняет функцию управления через контроль и коррекцию ошибок. Самостоятельная работа заключается в выполнении (как индивидуально, так и в команде) различного рода заданий в ходе внеаудиторной деятельности (самостоятельное прочтение, прослушивание, запоминание, осмысление и воспроизведение определенной информации). Данная работа выполняется в удобное для студентов время и представляется преподавателю на проверку. Самостоятельная работа предусматривает большую самостоятельность студентов, творческий и индивидуальный подход. Со стороны преподавателя – консультационная, контролирующая, психолого-педагогическая инновационная деятельность. Общими задачами самостоятельной работы студента являются:

–систематизация и закрепление полученных теоретических знаний и практических умений;

.

–углубление и расширение теоретических знаний;

–формирование навыков работы с литературой;

–развитие познавательных способностей и активности: творческой инициативы, самостоятельности, ответственности и организованности;

–формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

–развитие исследовательских умений.

Успешность самостоятельной работы определяется рядом условий, к которым можно отнести:

– целенаправленное планирование и рациональную организацию;

– мотивированность обучающихся на выполнение заданий;

– эффективную консультационную помощь;

– разнообразие видов и форм самостоятельной работы;

– обеспечение обучающихся необходимыми методическими и информационными ресурсами с целью превращения самостоятельной работы в творческий процесс.

Анализ самостоятельной работы студента за период обучения по дисциплине предполагает высокий уровень рефлексии и ответы на следующие вопросы:

- каковы достижения и неудачи в самостоятельной работе; в чем их причины?
- какие компетенции общекультурные и профессиональные удалось развить (сформировать)?
- какие учебные и личностные достижения сопутствовали данному этапу обучения?
- какие виды самообразовательной деятельности в данной предметной области будут способствовать личностному и профессиональному росту студента?

.

Контроль самостоятельной работы не должен быть исключительно формальным, поскольку именно на его основе, по сути, формируются последующие образовательные достижения студентов.

При изучении дисциплины «Защита информации» студентам предлагаются следующие формы самостоятельной работы:

- Подготовка к лекциям, а также их разбор, корректировка, изучение конспектов лекций;
- Изучение теоретического материала по учебникам, литературным и иным источникам (в библиотеках, дома, в компьютерном классе или др.);
- Подготовка ответов на вопросы лабораторных работ;
- Самостоятельное изучение отдельных тем (вопросов), составление конспекта;
- Подготовка к лабораторным работам;
- Подготовка к консультациям и их посещение по расписанию преподавателей;
- Подготовка к промежуточной аттестации.

Примерный перечень вопросов для собеседования (опроса) по дисциплине «Защита информации» по разделам дисциплины

ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Понятие информационной безопасности и её составляющие
2. Основные определения и критерии классификации угроз (примеры)
3. Процедурный уровень информационной безопасности (классы мер)
4. Основные понятия программно-технического уровня информационной безопасности
5. Особенности современных информационных систем, существенные с точки зрения безопасности
6. Архитектурная безопасность (особенности использования современных решений)
7. Идентификация и аутентификация
8. Протоколирование и аудит, шифрование, контроль целостности

.

9. Примеры решений для обеспечения информационной безопасности на предприятия
10. SIEM системы
11. Облачные технологии, примеры, сценарии использования

Перечень заданий для самостоятельного выполнения

Выполнить задания

Задание 1. Провести поиск информации на тему угроз информационной безопасности, сделать обзор и выявить наиболее эффективные способы минимизации рисков информационной безопасности

Задание 2. Проведение обследования информационной безопасности предприятий

Задание 3. Разработать концепцию информационной безопасности компании по следующему примерному плану

1. Цели системы информационной безопасности
2. Задачи системы информационной безопасности.
3. Объекты информационной безопасности.
4. Вероятные нарушители.
5. Основные виды угроз информационной безопасности.
6. Классификация угроз.

a. Основные непреднамеренные искусственные угрозы.
b. Основные преднамеренные искусственные угрозы.

7. Мероприятия по обеспечению информационной безопасности.
8. Средства защиты от потенциальных угроз.

Разработайте вариант политики паролей

Предложите ПО для антивирусной защиты (проведя сравнительный анализ цен, возможностей и пр)

Приложение 2

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

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Защита информации
«Специальность: 38.05.01 Экономическая безопасность
Специализация: «Экономико-правовое обеспечение экономической безопасности».
Форма подготовки очная

Владивосток
2018

Паспорт
фонда оценочных средств
по дисциплине
«Защита информации»

Код и формулировка компетенции	Этапы формирования компетенции	
ОК-8 - способность принимать оптимальные организационно-управленческие решения	Знает	Основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации для принятия оптимальных организационно-управленческих решений
	Умеет	Применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
	Владеет	Навыками работы с различными информационными ресурсами и технологиями
ПК-1 - способность подготавливать исходные данные, необходимые для расчета экономических показателей, характеризующих деятельность хозяйствующих субъектов	Знает	Методы подготовки исходных данных, необходимых для расчета экономических показателей, характеризующих деятельность хозяйствующих субъектов
	Умеет	Собирать и анализировать исходные данные для расчетов, прогнозировать угрозы информационной безопасности
	Владеет	Инструментами исследования и обобщения причин и последствий, выявленных в результате контроля отклонений, нарушений и недостатков
ПСК-1 - способность исследовать и обобщать причины и последствия, выявленные в результате контроля отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение	Знает	Методы контроля отклонений, нарушений и недостатков и приемы подготовки предложений, направленных на их устранение
	Умеет	Собирать и анализировать исходные данные для расчетов, прогнозировать угрозы информационной безопасности
	Владеет	Инструментами исследования и обобщения причин, выявленных в результате контроля отклонений, нарушений и недостатков

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ, ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ Тема 1, 2 Раздел 2. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (8 часов) Тема 1, 2	ОК-12	Основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	конспект (ПР-7); практическая работа (ПР-6)	Вопросы к зачету 1, 4
			Применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	практическая работа (ПР-6)	Вопросы к зачету 1, 4
			Навыками работы с различными информационными ресурсами и технологиями	практическая работа (ПР-6); контрольная работа (ПР-2)	Вопросы к зачету 1, 4
2	Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Тема 1, 2	ПСК-1	Методы контроля отклонений, нарушений и недостатков и Приемы подготовки предложений, направленных на их устранение	конспект (ПР-7); практическая работа (ПР-6)	Вопросы к зачету 2,3,5,6,7,8

			Собирать и анализировать исходные данные для расчетов, прогнозировать угрозы информационной безопасности	практическая работа (ПР-6)	Вопросы к зачету 2,3,5,6,7,8
			Инструментами исследования и обобщения причин и последствий выявленных в результате контроля отклонений, нарушений и недостатков	практическая работа (ПР-6); контрольная работа (ПР-2); деловая игра (ПР-10)	Вопросы к зачету 2,3,5,6,7,8

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**Критерии**	**Показатели**
ОК-8 - способность принимать оптимальные организационно-управленческие решения ПК-1 - способность подготавливать исходные данные, необходимые для расчета экономических показателей, характеризующих деятельность хозяйствующих субъектов	знает (пороговый уровень)	роль и место информационной безопасности в системе национальной безопасности страны; угрозы информационной безопасности государства, организации, гражданина	Знание основных понятия информационной безопасности	- Способность дать общую характеристику информационной безопасности в системе национальной безопасности страны
	умеет (продвинутый)	выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;	Умение применять информационно-коммуникационные технологии для выявления угроз	- Способность выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
	владеет (высокий)	устойчивыми навыками решения профессиональных задач на основе информационно-коммуникационных технологий с учетом основных требований информационной безопасности	Навыками эффективного использования информационно-коммуникационных технологии для защиты информации	- Способность самостоятельного решения профессиональных задач на основе ИКТ с учетом основных требований информационной безопасности
ПСК-1 - способностью исследовать и обобщать причины и последствия выявленных в результате контроля отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение	знает (пороговый уровень)	современные подходы к построению систем защиты информации; компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Знание основных технических средств и информационных технологий и их возможностей для решения аналитических и исследовательских задач	- Способность охарактеризовать технические средства и информационные технологии и их возможности для решения аналитических и исследовательских задач
	умеет (продвинутый)	осуществлять основные приемы работы на персональном компьютере с учетом требований информационной безопасности	Умение обрабатывать информацию с помощью современных технических средств и информационных технологий	- Способность обрабатывать информацию с помощью современных технических средств и информационных технологий
	владеет (вы-	навыками работы с компьютерными программами,	Владение широким спектром современных	- Способность владеть широким спектром

	сокий)	инструментами и методами для обработки экономических данных и их интерпретации	методов и приёмов для эффективной обработки информации с помощью современных технических средств и информационных технологий	современных методов и приёмов для эффективной обработки информации с помощью современных технических средств и информационных технологий

Оценочные средства для проверки сформированности компетенций по дисциплине «Защита информации»

Код и формулировка компетенции	Задание
ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Найти ГОСТ Р ИСО/МЭК 27005-2010 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности", ознакомиться с его разделами. Сделать подборку уязвимостей системы защиты информационных активов.
ОПК-3 - способность работать с компьютером как средством управления информацией, работать с информацией из различных источников, в том числе в глобальных компьютерных сетях	Выберите три различных информационных актива организации (банк, ресторан, поликлиника, университет).
ПК-3 способность выбирать рациональные информационные системы и информационно-коммуникативных технологии решения для управления бизнесом	1. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов. 2. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 1 уязвимости.

Зачетационные материалы (оценочные средства по промежуточной аттестации и критерии оценки)

Вопросы к зачету

1. Понятие информационной безопасности и её составляющие

2. Основные определения и критерии классификации угроз (примеры)

3. Процедурный уровень информационной безопасности (классы мер)

.

4. Основные понятия программно-технического уровня информационной безопасности
5. Особенности современных информационных систем, существенные с точки зрения безопасности
6. Архитектурная безопасность (особенности использования современных решений)
7. Идентификация и аутентификация
8. Протоколирование и аудит, шифрование, контроль целостности
9. Примеры решений для обеспечения информационной безопасности на предприятия
10. SIEM системы
11. Облачные технологии, примеры, сценарии использования

Критерии выставления оценки студенту на зачете по дисциплине «Защита информации»

Баллы (рейтинговой оценки)	**Оценка зачёта/ зачета** (стандартная)	**Требования к сформированным компетенциям**
86-100	*«зачтено»/ «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.
76-85	*«зачтено»/ «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 выпол-

Баллы (рейтинговой оценки)	**Оценка зачёта/ зачета** (стандартная)	**Требования к сформированным компетенциям**
		нения.
75-61	*«зачтено»/ «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 ответах на дополнительные вопросы.
менее 61	*«не зачтено»/ «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 (типовые ОС по текущей аттестации и критерии оценки по каждому виду аттестации по дисциплине «Защита информации»)

Типовые оценочные средства по текущей аттестации по дисциплине «Защита информации» размещены в разделе рабочей учебной программы дисциплины «Учебно-методическое обеспечение самостоятельной работы обучающихся».

Критерии оценки выполнения аналитического задания

№ п/п	Критерий	Количество баллов
1	Готовность результатов самостоятельной работы в срок	30
2	Файл с результатами работы	70
	ИТОГО	100

Критерии оценки выполнения коллективного научно-исследовательского, творческого задания

№ п/п	Критерий	Количество баллов
1	Готовность результатов самостоятельной работы в срок	20
2	Материал современный, актуальный	20

№ п/п	Критерий	Количество баллов
3	Применен широкий спектр математических и статистических функций	40
4	Дополнительные баллы	20
	ИТОГО	100

Критерии оценки выполнения задания 3

№ п/п	Критерий	Количество баллов
1	Готовность результатов самостоятельной работы в срок	20
2	Использование широкого спектра программного обеспечения для обеспечения информационной безопасности	60
3	Дополнительные баллы	20
	ИТОГО	100

Критерии оценки выполнения коллективного задания

№ п/п	Критерий	Количество баллов
1	Готовность результатов самостоятельной работы в срок	20
2	Выполнение всех поставленных задач	60
3	Дополнительные баллы	20
	ИТОГО	100

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Текущая аттестация студентов. Текущая аттестация студентов по дисциплине «Защита информации» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация по дисциплине «Защита информации» проводится в форме контрольных мероприятий (тесты, практические занятия, практические задания) 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 (активность в ходе обсуждений материалов лекций, активное участие в дискуссиях с аргументами из дополнительных источников, внимательность, способность задавать встречные вопросы в рамках дискуссии или обсуждения, заинтересованность изучаемыми материалами);
- уровень овладения практическими умениями и навыками по всем видам учебной работы (определяется по результатам контрольных работ, практических занятий, ответов на тесты);
- результаты самостоятельной работы (задания и критерии оценки размещены в Приложении 1).

Промежуточная аттестация студентов. Промежуточная аттестация студентов по дисциплине «Защита информации» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Вид промежуточной аттестации – зачет (7 семестр), состоящий из устного опроса в форме собеседования и индивидуальных заданий.