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

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

СОГЛАСОВАНО

Руководитель ОП

_____ Е.Г. Юрченко

«__14__» __сентября__ 2017 г.

УТВЕРЖДАЮ

Заведующий кафедрой бизнес-информатики и экономико-математических методов

_____ Ю.Д. Шмидт

«__14__» __сентября__ 2017 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Обеспечение информационной безопасности бизнес-процессов»

Направление подготовки 38.03.05 Бизнес-информатика
Форма подготовки: очная

курс 4 семестр 7
лекции - 36 час.
лабораторные работы – 36 час.
в том числе с использованием МАО лек.__-_ _/лаб 18 час.
всего часов аудиторной нагрузки - 72 час.
в том числе с использованием МАО 18 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 45 час.
контрольные работы (количество) - 0
курсовая работа / курсовой проект -
зачет –
экзамен - 7 семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от___21.10.2016___ №___12-13-2030___

Рабочая программа обсуждена на заседании кафедры бизнес-информатики и экономико-математических методов, протокол № _7_ от «__14__» __сентября___2017 г.

Заведующий кафедрой: д-р экон. наук, проф. Ю.Д. Шмидт
Составитель: старший преподаватель В.В. Ерофеев

.

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «__17__» _____июня____ 2019 г. № __6__

Заведующий кафедрой _____ Ю.Д. Шмидт

(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 201 г. № _____

Заведующий кафедрой _____ **Ю.Д. Шмидт**

(подпись) (И.О. Фамилия)

.

ABSTRACT

Bachelor's degree in 38.03.05 Business Informatics.

Course title: Ensuring information security of business processes.

Variable part of Block 1, 4 credits.

Instructor: Erofeev Vladimir Vladimirovich, Senior Teacher.

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

- the ability to solve socio-economic problems and processes in solving professional problems using systems analysis methods and mathematical modeling;
- the ability to use modern methods and technologies (including information) in professional activities.

Learning outcomes:

general competences (GPC):

– ability to solve standard tasks of professional activity on the basis of information and bibliographic culture with the use of information and communication technologies and taking into account the basic information security requirements (GPC-1);

– ability to work with a computer as a means of information management, work with information from various sources, including global computer networks (GPC-3);

professional competences (PC):

– the ability to choose rational information systems and information and communication technology solutions for business management (PC-3).

Course description:

Information security, information security. Confidentiality, integrity, availability of information. Basic definitions and criteria for the classification of threats. The source of the threat attack. Unintended user errors. Malicious software. Interception of data.

.

Features of modern information systems, essential from a security point of view. Client-server architecture, external services, Microsoft Azure cloud platforms, Amazon EC2. SIEM systems.

Main course literature:

1. Grishina N.V. Informatscionnaya bezopasnost predpriyatia [Enterprise Information Security. Tutorial. M.:Forum, 2015. 238p]

(rus) – Access http://lib.dvfu.ru:8080/lib/item?id=chamo:795581&theme=FEFU

2. Gromov Y. Y., Drachev V.O., Ivanova O.G. Informatscionnaya bezopasnost I zaschita informatscii [Information Security and Information Security. Tutorial. Stariy Oskol.:TNT, 2015. 383p]

(rus) – Access http://lib.dvfu.ru:8080/lib/item?id=chamo:777045&theme=FEFU

3. Andrianov V.V., Zefirov S.L., Golovanov V.B. Obespechenie informatscionnoi bezopasnosti biznesa [Ensuring business information security. Tutorial. M.: CHIPSR, 2011. 373p

(rus) – Access http://www.iprbookshop.ru/38525.html

4. Chuyanov A.G. Obespechenie informatscionnoi bezopasnosti v komputernih sistemah [Ensuring information security in computer systems] Tutorial. Omsk.:, 2012. 204 p (rus) – Access http://www.iprbookshop.ru/36015.html

5. Gvozdeva V.A. Bazovie i prikladnie informazonnie tehnologii [Basic and applied information technologies. Tutorial. M.: INFRA-M, 2015. 384 p.] (rus) – Access http://znanium.com/catalog/product/504788

Form of final control: exam

.

Аннотация к рабочей программе дисциплины
«Обеспечение информационной безопасности бизнес-процессов»

Учебный курс «Обеспечение информационной безопасности бизнес-процессов» предназначен для студентов направления подготовки 38.03.05 Бизнес-информатика.

Дисциплина «Обеспечение информационной безопасности бизнес-процессов» включена в состав обязательных дисциплин вариативной части блока «Дисциплины (модули)».

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа. Учебным планом предусмотрены лекционные занятия (36 часов), лабораторные работы (36 часов, в том числе МАО 18 часов), самостоятельная работа (72 часа, в том числе 45 часа на подготовку к экзамену). Дисциплина реализуется на 4 курсе в 7 семестре.

Дисциплина «Обеспечение информационной безопасности бизнес-процессов» основывается на знаниях, умениях и навыках, полученных в результате изучения дисциплин «Информационные технологии в профессиональной деятельности», «Основы программирования для экономистов», «Базы данных и знаний в экономике», «Моделирование бизнес-процессов» и позволяет подготовить студентов к освоению ряда таких дисциплин, как «Информационные технологии – инфраструктура предприятия», «Управление разработкой информационных систем», «Управление ИТ-сервисами и контентом».

Содержание дисциплины состоит из четырех разделов и охватывает следующий круг вопросов:

1. Понятие информационной безопасности. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности.
2. Угрозы информационной безопасности. Критерии классификации угроз

.

3. Стандарты и спецификации в области информационной безопасности. Основные понятия. Механизмы безопасности. Классы безопасности.
4. Управление рисками. Подготовительные этапы. Идентификация рисков.
5. Уровни информационной безопасности. 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
6. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектура клиент-сервер, внешние сервисы, облачные платформы Microsoft Azure, Amazon EC2. SIEM системы.

Цель - подготовка бакалавров, которые смогут обеспечивать безопасность и целостность данных информационных систем и технологий, снижать риски информационной безопасности при проектировании, внедрении информационных систем.

Задачи:

- изучение основных составляющих информационной безопасности;
- ознакомление с угрозами информационной безопасности и их классификация;
- освоение способов и мер минимизации рисков;
- ознакомление с особенностями современных информационных систем с точки зрения информационной безопасности;

Для успешного изучения дисциплины «Обеспечение информационной безопасности бизнес-процессов» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность при решении профессиональных задач анализировать социально-экономические проблемы и процессы с применением методов системного анализа и математического моделирования;

.

- умение выполнять технико-экономическое обоснование проектов по совершенствованию и регламентацию бизнес-процессов и ИТ-инфраструктуры предприятия с точки зрения информационной безопасности;
- способность обеспечивать безопасность и целостность данных информационных систем.

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
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	Знает	основные понятия информационных технологий; понятия автоматизации информационных процессов в управлении; понятие информационной безопасности и ее составляющие; средства и возможности операционных систем современных ПЭВМ для решения задач обработки экономической информации.
	Умеет	использовать математические, статистические и количественные методы решения типовых организационно-управленческих задач; оформлять техническую документацию.
	Владеет	практическими навыками по программированию вычислительных процессов для решения экономических и расчетных задач.
ОПК-3 - способность работать с компьютером как средством управления информацией, работать с информацией из различных источников, в том числе в глобальных компьютерных сетях	Знает	задачи информационной безопасности; принципы построения современных информационных технологий; современное состояние и тенденции развития информационных технологий.
	Умеет	использовать для организации, хранения, поиска и обработки информации системы управления базами данных; применять на практике навыки работы с универсальными пакетами прикладных программ для решения управленческих задач; использовать для представления сведений об информационных моделях рабочих мест технологии гипертекста, баз данных, мультимедиа.
	Владеет	информационной культурой, навыками самостоятельного и грамотного поиска информации с применением автоматизированных информационных технологий.
ПК-3 способность вы-	Знает	методы выбора средств обеспечения информаци-

бирать рациональные информационные системы и информационно-коммуникативных технологии решения для управления бизнесом		онной безопасности бизнес процессов
	Умеет	использовать системы и средства информационной безопасности в управлении бизнесом
	Владеет	средствами обеспечения информационной безопасности бизнес процессов

Для формирования вышеуказанных компетенций в рамках дисциплины «Обеспечение информационной безопасности бизнес-процессов» применяются следующие методы активного/интерактивного обучения: демонстрация работы облачных технологий Microsoft Azure, разработка проекта информационной безопасности предприятия.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ (16 час)

Тема 1. Понятие информационной безопасности. Основные составляющие информационной безопасности (4 часа)

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

Тема 2. Угрозы информационной безопасности АС (12 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 (8 часов)

Тема 1. Законодательный уровень информационной безопасности (4 часа)

.

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

Тема 2. Понятие стандарта в области информационной безопасности (4 часа)

Основные понятия. Механизмы безопасности. Классы безопасности.

Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (12 час)

Тема 1. Управление рисками (4 часа)

Управление рисками. Подготовительные этапы. Идентификация рисков.

Тема 2. Уровни информационной безопасности (4 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 (4 часа)

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

.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

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

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

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

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

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

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

Лабораторная 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 «Обеспечение информационной безопасности бизнес-процессов» 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	ОПК-1	Основные понятия информационной безопасноти	конспект (ПР-7); лабораторная работа (ПР-6)	Вопросы к экзамену 1, 4
			Применять информационно-коммуникационные технологии для выявления угроз	лабораторная работа (ПР-6)	Вопросы к экзамену 1, 4
			Навыками эффективного использования информационно-коммуникационных технологии для защиты информации	лабораторная работа (ПР-6); контрольная работа (ПР-2)	Вопросы к экзамену 1, 4
2	Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Тема 1, 2	ОПК-3	Основные технические средства и информационные технологии и их возможности для решения аналитических и исследовательских задач	конспект (ПР-7); лабораторная работа (ПР-6)	Вопросы к экзамену 2,3,5,6,7,8
			Обрабатывать информацию с помощью современных технических средств и информационных технологий	лабораторная работа (ПР-6)	Вопросы к экзамену 2,3,5,6,7,8
			Широким спектром современных методов и приёмов для эффективной обработки информации с помощью современных технических средств и информационных технологий	лабораторная работа (ПР-6); контрольная работа (ПР-2); деловая игра (ПР-10)	Вопросы к экзамену 2,3,5,6,7,8
3	Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Тема 3	ПК-19	Основные технические средства и информационные технологии, применяемые для защиты бизнес-процессов предприятия	конспект (ПР-7); лабораторная работа (ПР-6)	Вопросы к экзамену 9, 10, 11
			Применять основные технические средства и информационные технологии в целях минимизации угроз	лабораторная работа (ПР-6)	Вопросы к экзамену 9, 10, 11
			Широким спектром современных передовых технических средстви информационные технологии для информационной безопаности	лабораторная работа (ПР-6); контрольная работа (ПР-2)	Вопросы к экзамену 9, 10, 11

.

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)
(печатные и электронные издания)

1. Андрианов В. В., Обеспечение информационной безопасности бизнеса [Электронный ресурс]/ В.В. Андрианов [и др.].— Электрон. текстовые данные.— М.: ЦИПСиР, 2011.— 373 с.— Режим доступа: http://www.iprbookshop.ru/38525.html
2. Гришина Н.В. Информационная безопасность предприятия : учебное пособие для вузов / Н. В. Гришина. Москва : Форум, 2015. 238с. Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:795581&theme=FEFU
3. Громов Ю.Ю., Драчев В.О., Иванова О.Г. Информационная безопасность и защита информации : учебное пособие для вузов / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. Старый Оскол : ТНТ, 2015. 383с. Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:777045&theme=FEFU
4. Гвоздева, Т.В. Проектирование информационных систем: Учебное пособие / Т.В. Гвоздева, Б. А. Баллод. - Ростов-на-Дону, Феникс, 2009. - 512 с. Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:292742&theme=FEFU
5. Голицына, О.Л. Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - М.: Форум, 2009. - 496 с. Ре-

жим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:268425&theme=FEFU

6. Грекул, В. И. Проектирование информационных систем : Учебное пособие / В. И. Грекул, Г. Н. Денищенко, Н. Л. Коровкина. – М.: ИНТУИТ. БИНОМ. ЛЗ, 2008. – 300 с. Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:274425&theme=FEFU
7. Чуянов А.Г., Симаков А.А. ,Обеспечение информационной безопасности в компьютерных системах [Электронный ресурс]: учебное пособие/ Чуянов А.Г., Симаков А.А.— Электрон. текстовые данные.— Омск: Омская академия МВД России, 2012.— 204 c. Режим доступа: http://www.iprbookshop.ru/36015.html

Дополнительная литература

(печатные и электронные издания)

1. ГОСТ 34.003-90. Автоматизированные системы. Термины и определения.

2. Федеральный закон N 152-ФЗ "О персональных данных"

3. Абдикеева, Н.М. Корпоративные информационные системы управления: Учебник / Под науч. ред. Н.М. Абдикеева, О.В. Китовой. - М.: ИНФРА-М, 2011. – 464 с.

4. Балдин, К.В. Информационные системы в экономике: Учебное пособие / К.В. Балдин. - М.: НИЦ Инфра-М, 2013. - 218 с.

5. Карминский, А.М. Применение информационных систем в экономике: Учебное пособие / А.М. Карминский, Б.В. Черников. - 2-е изд., перераб. и доп. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 320 с.

6. Мартишин, С.А. Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench: Учебное пособие / С.А. Мартишин и др. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2012. - 160 с

7. Федотова, Е.Л. Информационные технологии и системы: Учеб. пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 352 с.

8. Зинченко, Б. Универсальное представление моделей бизнес-процессов / Б.Зинченко, Х-Ю.Шерер // Инвестиции в России. - 2011. - № 2. - с. 27-35.

9. https://www.intuit.ru/studies/courses/30/30/info Галатенко В..А., Стандарты информационной безопасности

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Клементьев, И.П. Введение в Облачные вычисления / И.П. Клементьев, В.А. Устинов. – М. : Интуит, 2012. – 233 с. [Электронный ресурс]. – Режим доступа : http://www.kodges.ru/komp/program/129905-vvedenie-v-oblachnye-vychisleniya.html.
2. Фингар, П. DOT.CLOUD. Облачные вычисления – бизнес-платформа XXI века / П. Фигнар. – М. : Аквамариновая Книга, – 256 с. [Электронный ресурс]. – Режим доступа : http://www.kodges.ru/komp/132940-oblachnye-vychisleniya-biznes-platforma-xxi-veka.html.
3. Электронная библиотека и базы данных ДВФУ. http://dvfu.ru/web/library/elib
4. Электронно-библиотечная система «Лань» http://e.lanbook.com
5. Электронно-библиотечная система «Научно-издательского центра ИНФРА-М» http://znanium.com
6. Электронно-библиотечная система БиблиоТех. http://www.bibliotech.ru
7. Электронный каталог научной библиотеки ДВФУ http://lib.dvfu.ru:8080/search/query?theme=FEFU
8. Научная библиотека КиберЛенинка: http://cyberleninka.ru/

Перечень информационных технологий и программного обеспечения

Перечень информационных технологий и программного обеспечения дисциплины «Обеспечение информационной безопасности бизнес-процессов» 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 «Обеспечение информационной безопасности бизнес-процессов» предусматривает следующие виды учебной работы: лекции, лабораторные работы, самостоятельную работу студентов, текущий контроль и промежуточную аттестацию.

Освоение курса дисциплины «Обеспечение информационной безопасности бизнес-процессов» 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 «Обеспечение информационной безопасности бизнес-процессов» является экзамен, 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 «Обеспечение информационной безопасности бизнес-процессов» при условии выполнения всех видов текущего контроля и самостоятельной работы, предусмотренных учебной программой.

Критерии оценки по дисциплине «Обеспечение информационной безопасности бизнес-процессов» для аттестации на экзамене 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 времени, 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 лабораторной 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 маши-

нами, 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 ОБРАЗОВАНИЯ И НАУКИ 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 «Обеспечение информационной безопасности бизнес-процессов»

Направление подготовки 38.03.05 Бизнес-информатика

Форма подготовки: очная

Владивосток
2017

.

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;	(0,5 час в неделю) 9 часов	Опрос Собеседование
2	В течение семестра	Подготовка к лабораторным работам	(1 час в неделю) 18 часов	Сдача работы
3	В течение семестра	Подготовка к экзамену	45часов	Собеседование
		Итого	72 часа	

Методические 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 лабораторной работы по дисциплине «Обеспечение информационной безопасности бизнес-процессов» 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 экзамену

Экзамен – это заключительный этап изучения дисциплины «Обеспечение информационной безопасности бизнес-процессов», имеющий целью проверить теоретические знания студента, его навыки и умение применять полученные знания при решении практических задач. Экзамен проводится в объеме учебной программы по дисциплине в устной форме.

Подготовка к экзамену 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 «Обеспечение информационной безопасности бизнес-процессов» разбита на разделы, которые представляют собой логически завершенные части рабочей программы курса и являются тем комплексом знаний и умений, которые подлежат контролю.

.

Лекции и лабораторные работы являются важными этапами подготовки к экзамену, 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, лабораторные работы);
- своевременно выполнять лабораторные 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 «Обеспечение информационной безопасности бизнес-процессов» становится залогом получения высокой оценки знаний (в соответствии с рейтинговой системой оценок).

Таким образом, экзамен выставляется без опроса – по результатам работы студента в течение семестра. Для этого студенту необходимо посетить все лекционные и лабораторные занятия, активно работать на них, устно доказать знание основных понятий и терминов по дисциплине «Обеспечение информационной безопасности бизнес-процессов».

Студенты, не прошедшие по рейтингу, готовятся к экзамену согласно вопросам к экзамену, на котором должны показать, что материал курса ими освоен. При подготовке к экзамену 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).

В экзаменационном билете по дисциплине «Обеспечение информационной безопасности бизнес-процессов» предлагается два задания в виде во-

просов, носящих теоретический. Время на подготовку к экзамену 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 экзамена.

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 «Обеспечение информационной безопасности бизнес-процессов» 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 (экзамен в 6 семестре).

Примерный перечень вопросов для собеседования (опроса) по дисциплине «Обеспечение информационной безопасности бизнес-процессов» по разделам дисциплины

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

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

«Обеспечение информационной безопасности бизнес-процессов»

Направление подготовки 38.03.05 Бизнес-информатика

Форма подготовки: очная

Владивосток
2017

Паспорт
фонда оценочных средств
по дисциплине
«Обеспечение информационной безопасности бизнес-процессов»

Код и формулировка компетенции	Этапы формирования компетенции	
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	знает	основные понятия информационных технологий; понятия автоматизации информационных процессов в управлении; понятие информационной безопасности и ее составляющие; средства и возможности операционных систем современных ПЭВМ для решения задач обработки экономической информации.
	умеет	использовать математические, статистические и количественные методы решения типовых организационно-управленческих задач; оформлять техническую документацию.
	владеет	навыками эффективного использования информационно-коммуникационных технологии для решения задач экономического характера
ОПК-3 - способность работать с компьютером как средством управления информацией, работать с информацией из различных источников, в том числе в глобальных компьютерных сетях	знает	задачи информационной безопасности; принципы построения современных информационных технологий; современное состояние и тенденции развития информационных технологий.
	умеет	использовать для организации, хранения, поиска и обработки информации системы управления базами данных; применять на практике навыки работы с универсальными пакетами прикладных программ для решения управленческих задач; использовать для представления сведений об информационных моделях рабочих мест технологии гипертекста, баз данных, мультимедиа.
	владеет	Широким спектром современных методов и приёмов для эффективной защиты информации с помощью современных технических средств и информационных технологий
ПК-3 способность выбирать рациональные информационные системы и информационно-коммуникативных технологии решения для управления бизнесом	знает	методы выбора средств обеспечения информационной безопасности бизнес процессов
	умеет	использовать системы и средства информационной безопасности в управлении бизнесом
	владеет	средствами обеспечения информационной безопасности бизнес процессов

№ 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	ОПК-1	Основные понятия информационной безопасности	конспект (ПР-7); лабораторная работа (ПР-6)	Вопросы к экзамену 1, 4
			Применять информационно-коммуникационные технологии для выявления угроз	лабораторная работа (ПР-6)	Вопросы к экзамену 1, 4
			Навыками эффективного использования информационно-коммуникационных технологии для защиты информации	лабораторная работа (ПР-6); контрольная работа (ПР-2)	Вопросы к экзамену 1, 4
2	Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Тема 1, 2	ОПК-3	Основные технические средства и информационные технологии и их возможности для решения аналитических и исследовательских задач	конспект (ПР-7); лабораторная работа (ПР-6)	Вопросы к экзамену 2,3,5,6,7,8
			Обрабатывать информацию с помощью современных технических средств и информационных технологий	лабораторная работа (ПР-6)	Вопросы к экзамену 2,3,5,6,7,8
			Широким спектром современных методов и приёмов для эффективной обработки информации с помощью современных технических средств и информационных технологий	лабораторная работа (ПР-6); контрольная работа (ПР-2); деловая игра (ПР-10)	Вопросы к экзамену 2,3,5,6,7,8
3	Раздел 3. УПРАВЛЕНИЕ РИСКАМИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Тема 3	ПК-19	Основные технические средства и информационные технологии, применяемые для защиты бизнес-процессов предприятия	конспект (ПР-7); лабораторная работа (ПР-6)	Вопросы к экзамену 9, 10, 11
			Применять основные технические средства и информационные технологии в целях минимизации угроз	лабораторная работа (ПР-6)	Вопросы к экзамену 9, 10, 11
			Широким спектром современных передовых технических средстви информационные технологии для информационной безопаности	лабораторная работа (ПР-6); контрольная работа (ПР-2)	Вопросы к экзамену 9, 10, 11

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	Этапы формирования компетенции		Критерии	Показатели
ОПК-1 - способность решать стандарт-	знает (пороговый	основные понятия информационных технологий; понятия автоматизации ин-	Знание основных понятия информационной безопасности	– Способность дать общую характеристику информационной без-

ные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	уровень)	формационных процессов в управлении; понятие информационной безопасности и ее составляющие; средства и возможности операционных систем современных ПЭВМ для решения задач обработки экономической информации.		опасности в системе национальной безопасности страны
	умеет (продвинутый)	использовать математические, статистические и количественные методы решения типовых организационно-управленческих задач; оформлять техническую документацию.	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)	навыками эффективного использования информационно-коммуникационных технологии для решения задач экономического характера	Навыками эффективного использования информационно-коммуникационных технологии для защиты информации	– Способность самостоятельного решения профессиональных задач на основе ИКТ с учетом основных требований информационной безопасности
ОПК-3 - способность работать с компьютером как средством управления информацией, работать с информацией из различных источников, в том числе в глобальных компьютерных сетях	знает (пороговый уровень)	задачи информационной безопасности; принципы построения современных информационных технологий; современное состояние и тенденции развития информационных технологий.	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)	использовать для организации, хранения, поиска и обработки информации системы управления базами данных; применять на практике навыки работы с универсальными пакетами прикладных программ для решения управленческих задач; использовать для представления сведений об информационных моделях рабочих мест технологии гипертекста, баз данных, мультимедиа.	Умение обрабатывать информацию с помощью современных технических средств и информационных технологий	– Способность обрабатывать информацию с помощью современных технических средств и информационных технологий
	владеет (высокий)	Широким спектром современных методов и приёмов для эффективной защиты информации с помощью современных технических средств и информационных технологий	Владение широким спектром современных методов и приёмов для эффективной обработки информации с помощью современных технических средств и информационных технологий	– Способность владеть широким спектром современных методов и приёмов для эффективной обработки информации с помощью современных технических средств и информационных технологий
ПК-3 способность выбирать рациональные информационные системы и ин-	знает (пороговый уровень)	методы выбора средств обеспечения информационной безопасности бизнес процессов	Знание основных технических средств и информационных технологий, применяемых для защиты бизнес-процессов	– Способность охарактеризовать основные технические средства и информационные технологиий, применяемые для защиты биз-

формационно-коммуникативных технологии решения для управления бизнесом			предприятия	нес-процессов предприятия
	умеет (продвинутый)	использовать системы и средства информационной безопасности в управлении бизнесом	Умение применять основные технические средства и информационные технологии в целях минимизации угроз	– Способность применять основные технические средства и информационные технологии в целях минимизации угроз.
	владеет (высокий)	средствами обеспечения информационной безопасности бизнес процессов	Владение широким спектром современных передовых технических средств и информационные технологии для информационной безопасности	– Способность управлять широким спектром современных передовых технических средств и информационные технологии для информационной безопасности

Оценочные средства для проверки сформированности компетенций по дисциплине «Обеспечение информационной безопасности бизнес-процессов»

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.

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

Вопросы к экзамену

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 экзамене по дисциплине «Обеспечение информационной безопасности бизнес-процессов»

Баллы (рейтинговой оценки)	**Оценка зачёта/ экзамена** (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 выполнения.
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 последователь-

		ности 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 «Обеспечение информационной безопасности бизнес-процессов»)

Типовые оценочные средства по текущей аттестации по дисциплине «Обеспечение информационной безопасности бизнес-процессов» 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
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

№ п/п	Критерий	Количество баллов
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 «Обеспечение информационной безопасности бизнес-процессов» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация по дисциплине «Обеспечение информационной безопасности бизнес-процессов» проводится в форме контрольных мероприятий (тесты, лабораторные 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 «Обеспечение информационной безопасности бизнес-процессов» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

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