МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования

«Дальневосточный федеральный университет»

(ДВФУ)

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

СОГЛАСОВАНО
Руководитель МОП
«Международный бизнес и управление проектами»

_____ Д.А. Соколова
(подпись) (Ф.И.О. рук. ОП)
«___» _____ 2018 г.

УТВЕРЖДАЮ
Заведующий кафедрой
Менеджмента

_____ Е.А. Глотова
(подпись) (Ф.И.О. зав. каф.)
«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Кибербезопасность (CyberSecurity)

Направление подготовки 38.04.02 Менеджмент

Магистерская программа «Международный бизнес и управление проектами»

Форма подготовки: очная

курс __2_____ семестр __3_____
лекции _18_ час.
практические занятия__36___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 __54_____ час.
в том числе на подготовку к экзамену __0____ час.
контрольные работы (количество) – не предусмотрены
курсовая работа / курсовой проект _____ семестр
зачет __3___ семестр
экзамен _____семестр

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 менеджмента, протокол № ??? от «????» _____ 201? г.

Заведующий кафедрой: д-р полит. наук, проф. Глотова Е.А.
Составители: магистр эконом. наук. Лутченко В.А.

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)

ABSTRACT

Master's degree in 38.04.02 Management / International Business and Project Management.

Course title: CyberSecurity.

Variable part of Block 3 credits.

Instructor: Lutchenko Valeriia Alekseevna, Master degree of Economic Sciences, Assistant of Management Department & Finance and Credits Department.

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

- ability to self-organization and self-education;
- 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.

Learning outcomes:

General Competences (GC):

- the ability to use modern methods of corporate finance management for solving strategic tasks (GC-3);
- possession of methods of economic and strategic analysis of the behavior of economic agents and markets in a global environment (GC-9).

Course description: the content of the discipline consists of three sections and covers the following range of issues:

1. Introduction to the problem of cyber security: information security of cybernetic systems; ensuring the safety of automated process control systems;

2. Features of cybernetic systems protection: main threats, vulnerabilities, security risks of the Internet of Things, Requirements for information protection systems when integrated with real-time systems and methods for economic and strategic analysis of the behavior of economic agents and markets in the global environment.

3. Technologies of network security threats: Basics of legal regulation of information protection of critical facilities and modern methods of corporate finance management for solving strategic tasks, mechanisms to counter network attacks.

Main course literature:

1. Richard Stiennon, Chief Research Analyst, IT-Harvest, National Fintech Cybersecurity Summit 2016.
2. “Hackers Use New Tactic at Austrian Hotel: Locking the Doors,” NYTimes.com, Jan 2017, https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html.
3. “Target Hackers Broke in Via HVAC Company,” KrebsonSecurity.com, Feb 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Form of final control: pass/fail exam.

Аннотация к рабочей программе
дисциплины «Cybersecurity (Кибербезопасность)»

Учебный курс «Cybersecurity (Кибербезопасность)» предназначен для студентов направления подготовки 38.04.02 Менеджмент, магистерская программа «International Business and Project Management / Международный бизнес и управление проектами (на английском языке)».

Дисциплина «Cybersecurity (Кибербезопасность)» включена в состав дисциплин по выбору вариативной части блока «Дисциплины (модули).

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов. Учебным планом предусмотрены лекционные занятия (18 часов), практические занятия (36 часов, в том числе МАО 18 часов), самостоятельная работа (54 часа). Дисциплина реализуется на 2 курсе в 3 семестре.

Дисциплина «Cybersecurity (Кибербезопасность)» основывается на знаниях, умениях и навыках, полученных в результате изучения дисциплин «Управление проектами», «Теория организации и организационное поведение», «Управленческая экономика» и позволяет подготовить студентов к освоению ряда таких дисциплин, как «Маркетинговое управление», «Менеджмент качества при создании инновационных продуктов» и «Strategic Management (Стратегический менеджмент)».

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

1. Введение в проблему кибербезопасности: информационная безопасность кибернетических систем; обеспечение безопасности автоматизированных систем управления технологическими процессами;

2. Особенности защиты кибернетических систем: основные угрозы, уязвимости, риски в области безопасности Интернета вещей, Требования к системам защиты информации при интеграции с системами реального времени и методы экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.

3. Технологии угроз сетевой безопасности: Основы правового регулирования защиты информации критически важных объектов и современные методы управления корпоративными финансами для решения стратегических задач, механизмы противодействия сетевым атакам.

Цель – формирование у студентов системного представления о кибербезопасности, практических методах и инструментах обеспечения информационной безопасности, необходимых для эффективной работы в современном бизнес-пространстве.

Задачи:

- изучение понятийного аппарата дисциплины, основных теоретических положений и методов;
- формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач;
- формирование знаний теоретических основ в сфере обеспечения безопасности цифровой информации; этапы обеспечения информационной безопасности кибернетических систем, в том числе обеспечение безопасности автоматизированных систем управления технологическими процессами; технологии угроз сетевой безопасности, а также механизмы противодействия сетевым атакам;
- формирование у студентов профессиональных умений и навыков в области использования современных техник и международных стандартов в области оценивания текущих ситуаций и прогнозов будущих рисков, связанных с угрозами кибербезопасности; технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам.

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

- способность к логическому мышлению, анализу, систематизации,

обобщению, критическому осмыслению информации;

- способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач.
- способность к самосовершенствованию и саморазвитию в профессиональной сфере, к повышению общекультурного уровня;
- готовность интегрироваться в научное, образовательное, экономическое, политическое и культурное пространство России и АТР;
- способность проявлять инициативу и принимать ответственные решения, осознавая ответственность за результаты своей профессиональной деятельности;
- способность использовать современные методы и технологии (в том числе информационные) в профессиональной деятельности;
- способность к самоорганизации и самообразованию.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции:

Код и формулировка компетенции	**Этапы формирования компетенции**	
ПК-3 – способность использовать современные методы управления корпоративными финансами для решения стратегических задач;	знает	сущность решений защиты информации кибернетических систем; основы оценивания влияния средств защиты информации на критически важные экономические объекты информатизации.
	умеет	находить решения стандартных задач профессиональной деятельности на основе методов оптимизации систем защиты информации и управления корпоративными финансами для решения стратегических задач.
	владеет	способность формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.
ПК-9 владением методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде	знает	сущность методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.
	умеет	формировать требования для системы защиты информации, для систем реального времени с

	учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.
владеет	способность оценивать влияние средств защиты информации на критически важные экономические объекты информатизации.

Для формирования вышеуказанных компетенций в рамках дисциплины «Cybersecurity (Кибербезопасность)» применяются следующие методы активного/ интерактивного обучения: лекция-презентация, лекция-дискуссия, кейс-стади.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА (18 ЧАС.)

Раздел 1. Введение в проблему кибербезопасности. (6 час.)

Тема 1. Введение в проблему кибербезопасности. Введение в теорию доверенных систем (2 час.)

- Понятие кибербезопасности.
- Роль человека в кибернетических системах
- Проблема информационной безопасности в кибернетических системах
- Понятие доверенной информационной системы

Отношения доверия в информационных системах

Тема 2. Понятие критически важного объекта. Основы правового регулирования защиты информации критически важных объектов и современные методы управления корпоративными финансами для решения стратегических задач (4 час.)

- Понятие критически важного объекта
- Особенности функционирования критически важных объектов
- Требования к информационной безопасности критически важных экономических объектов
- Основы правового регулирования вопросов защиты информации на критически важных экономических объектах

Раздел 2. Особенности защиты кибернетических систем. (4 час.)

Тема 3. Особенности защиты кибернетических систем: Internet- вещей, smart things (4 час.)

- Кибернетические системы, характеристики, жизненный цикл, проблема сопровождения больших кибернетических систем в рамках поведения экономических агентов и рынков в глобальной среде
- Особенности эксплуатации, ограничения, связанные с длительными сроками эксплуатации систем Internet вещей, smart things – коммуникация и принятие решений без участия человека
- Требования к обеспечению безопасности управления корпоративными финансами для решения стратегических задач

<u>Раздел 3. Технологии угроз сетевой безопасности. (8 час.)</u>

Тема 4. Требования к системам защиты информации при интеграции с системами реального времени и методы экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде (4 час.)

- Определение систем реального времени с точки зрения информационной безопасности управления корпоративными финансами для решения стратегических задач
- Определение требований к обеспечению информационной безопасности экономических агентов и рынков в глобальной среде

Тема 5. Методологические рекомендации по анализу режимов работы Кибернетических систем управления корпоративными финансами для решения стратегических задач (4 час.)

- Степень влияния на систему в целом. Зависимость опасности выявленных уязвимостей от качества управления корпоративными финансами для решения стратегических задач
- Виды идентификации, применяемые в современных экономических условиях

- Понятие идентификационной сущности экономических агентов и рынков в глобальной среде
- Проблема хранения идентификационной сущности
- Процедуры идентификации без участия человека

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия
(36 час., в том числе 18 час. с использованием методов активного обучения (МАО))

Практическое занятие 1-2-3. Введение в проблему кибербезопасности. Введение в теорию доверенных систем (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (2 час.)

- Понятие кибербезопасности.
- Роль человека в кибернетических системах
- Проблема информационной безопасности в кибернетических системах
- Понятие доверенной информационной системы
- Отношения доверия в информационных системах
- Решение кейсов

Практическое занятие 4-5-6-8. Понятие критически важного объекта. Основы правового регулирования защиты информации критически важных объектов и современные методы управления корпоративными финансами для решения стратегических задач (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (4 час.)

- Понятие критически важного объекта
- Особенности функционирования критически важных объектов
- Требования к информационной безопасности критически важных экономических объектов
- Основы правового регулирования вопросов защиты информации на критически важных экономических объектах
- Решение кейсов

Практическое занятие 9-10-11. Особенности защиты кибернетических систем: Internet- вещей, smart things (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (6 час.)

- Кибернетические системы, характеристики, жизненный цикл, проблема сопровождения больших кибернетических систем в рамках поведения экономических агентов и рынков в глобальной среде
- Особенности эксплуатации, ограничения, связанные с длительными сроками эксплуатации систем Internet вещей, smart things – коммуникация и принятие решений без участия человека
- Требования к обеспечению безопасности управления корпоративными финансами для решения стратегических задач
- Решение кейсов

Практическое занятие 12-13. Требования к системам защиты информации при интеграции с системами реального времени и методы экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (4 час.)

- Определение систем реального времени с точки зрения информационной безопасности управления корпоративными финансами для решения стратегических задач
- Определение требований к обеспечению информационной безопасности экономических агентов и рынков в глобальной среде
- Решение кейсов

Практическое занятие 14-15. Методологические рекомендации по анализу режимов работы. Кибернетических систем управления корпоративными финансами для решения стратегических задач (4 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (2 час.)

- Степень влияния на систему в целом. Зависимость опасности выявленных уязвимостей от качества управления корпоративными финансами для решения стратегических задач
- Виды идентификации, применяемые в современных экономических условиях
- Понятие идентификационной сущности экономических агентов и рынков в глобальной среде
- Проблема хранения идентификационной сущности
- Процедуры идентификации без участия человека
- Решение кейсов

II. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Кибербезопасность» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение заданий;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы;
- критерии оценки выполнения самостоятельной работы.

III. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в проблему кибербезопасности - Раздел II. Особенности защиты кибернетических систем	ПК-3	Знает: сущность решений защиты информации кибернетических систем; основы оценивания влияния средств защиты информации на критически важные экономические объекты информатизации	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету 1-15.
			Умеет: находить решения стандартных задач профессиональной деятельности на основе методов оптимизации систем защиты информации и управления корпоративными финансами для решения стратегических задач	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету 1-15.
			Владеет: способностью формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету 1-15.
2	Раздел II. Особенности защиты кибернетических систем - Раздел III. Технологии угроз сетевой безопасности	ПК-9	Знает: сущность методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету 1-15.
			Умеет: формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету 1-15.

			экономического объекта защиты и рынков в глобальной среде.		
			Владеет: способность оценивать влияние средств защиты информации на критически важные экономические объекты информатизации.	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету 1-15.

Текущий контроль. Предусматривает учет посещения студентами занятий в течении периода обучения и оценку своевременности и качества выполнения студентами практических заданий и самостоятельных работ.

Пример практических заданий и типовые задания для самостоятельной работы, 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.

Итоговый контроль. Предусматривает рейтинговую оценку по учебной дисциплине в течении семестра в процессе обучения.

IV. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Richard Stiennon, Chief Research Analyst, IT-Harvest, National Fintech Cybersecurity Summit 2016.
2. “Hackers Use New Tactic at Austrian Hotel: Locking the Doors,” NYTimes.com, Jan 2017, https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html.

3. “Target Hackers Broke in Via HVAC Company,” KrebsonSecurity.com, Feb 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

Дополнительная литература:

(печатные и электронные издания)

1. Полянский, Дмитрий Александрович. Методы контроля и обеспечения достоверности информации в АСУП : автореф. дис. на соиск. учен. степ. канд. техн. наук : спец. 05.13.06 / Д. А. Полянский .— Владимир : [б. и.] 2010 .— 15 с. : ил. ; 21 см. — Библиогр.: с.14-15.

2. Гуц, Александр Константинович (д-р физ.-мат. наук). Теория игр и защита компьютерных систем [Текст] : [учебное пособие для студентов и аспирантов факультетов компьютерных наук и математических факультетов вузов] / А.К. Гуц, Т.В. Вахний ; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования Ом. гос. ун-т им. Ф.М. Достоевского .— Омск : Изд-во Омского гос. ун-та, 2013. — 159 с. : ил., портр., табл. ; 21 см. — Библиогр.: с.155-159 (66 назв.) .—ISBN 978-5-7779-1655-6, 150 экз. 3

3. Защита информации в информационных системах : учебное пособие для студентов высших учебных заведений, обучающихся по направлению "Информатика и вычислительная техника" и слушателей Программ профессиональной переподготовки и повышения квалификации специалистов Российской Федерации и стран СНГ по новым направлениям развития техники и технологии / И.В. Баскаков, В.Л. Евсеев, А.В. Пролетарский, А.М. Суворов ; [Гос. образоват. учреждение высш. проф. образования "Моск. гос. техн. ун-т им. Н.Э. Баумана"] .— Москва : Рудомино, 2011 .— 359 с. : ил. ; 20 см. — Дар Межгосударственного фонда гуманитарного сотрудничества государств-участников СНГ Библиотека Новосибирского государственного университета : 608816 .— Библиогр.: с.358-359 .— ISBN 978-5-905017-16-2, 500 экз.

4. Шаньгин, Владимир Федорович. Информационная [учебное пособие для студентов вузов] / В.Ф. Шаньгин .— Москва : ДМК, 2014 .— 701 с. : ил. ; 20 см .— (Администрирование и защита) .— Библиогр.: с.679-685 .— Предм. указ.: с.686-701 .— ISBN 978-5-94074-768-0 5 Операционная система реального времени QNX Neutrino 6.5.0. Системная архитектура : пер. с англ. / [гл. ред. Е. Кондукова] .— Санкт-Петербург : БХВ-Петербург, 2014 .— 388 с. : ил. ; 21 см. — Предм. указ.: с. 379-388 .— ISBN 978-5-9775-3350-8 : 1 000 экз.

5. One in two users click on links from unknown senders', Fau.eu, August 2016. www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-linksfrom-unknown-senders Fisher, C. (2007) *Researching and Writing a Dissertation for Business Students* (2nd edn), Harlow: Financial Times Prentice Hall. Chapter 1 has some very practical tips on choosing your research topic**.**

6. Alperovitch, D. (2011) "Revealed: Operation Shady RAT" McAfee Corporation Santa Clara, CA.

7. Chew, E., et al. (2008) Performance Measurement Guide for Information Security, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland.

8. Drew, D. M. and D. M. Snow (2006) Making Twenty-First-Century Strategy: An Introduction to Modern National Security Processes and Problems, Air University Press, Maxwell AFB, Alabama.

9. Parker, D. B. (1997) "The strategic value of information security in business", Computers & Security, 16 (7), pp. 572-582.

10. Powner, D. (2009) "National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture". in Testimony Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives, Washington, United States Government Accounting Office (GAO).

11. Rockefeller, J., E. Bayh, B. Nelson and O. Snowe (2009) "S. 773: Cybersecurity Act of 2009". in 111th Congress 2009-2010, Washington, DC, United States Senate Committee on Commerce, Science & Transportation.

12. Shanmugam, K. (2009) "Cooperating for Infocomm Security: Singapore Infocomm Technology Security Authority (or SITSA)" in The 18th Government ware Seminar, The Suntec Singapore International Convention and Exhibition Centre, Minister for Law and 2nd Minister for Home Affairs.

13. Sinks, M. A. (2008) Cyber Warfare and International Law, Air University, Alabama.

14. Sklenka, S. D. (2007) Strategy, National Interests, And Means to An End, Strategic Studies Institute, U.S. Army War College, Carlisle, PA.

15. Toure, H. (2010) "Securing Cyberspace". in Annual Meeting 2010 of the World Economic Forum, Davos, Switzerland, World Economic Forum.

16. Toure, H. (2010c) "Building Confidence and Security in the Use of ICTs". in Interactive Facilitation Meeting on WSIS Action Line C5: Cybersecurity (12 May 2010) - Speech by ITU Secretary-General, Dr. Hamadoun I. Toure, Geneva, Switzerland, International Telecommunication Union (ITU).

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Freedom Collection на портале ScienceDirect http://www.sciencedirect.com/

2. Электронная библиотека и базы данных ДВФУ . http://dvfu.ru/web/library/elib

3. Электронно-библиотечная система «Научно-издательского центра ИНФРА-М» http://znanium.com

4. Электронно-библиотечная система Российской государственной библиотеки им.Ленина. http://www.rgb.ru

5. Научная библиотека КиберЛенинка: http://cyberleninka.ru/

6. НГУ. Электронная библиотека http://libra.nsu.ru/catalogue/;
7. НГУ. Научная электронная библиотека http://libra.nsu.ru/scientificres/
8. Электронно-библиотечная система «Лань» http://e.lanbook.com/
9. Официальный сайт Федеральной службы по техническом и
10. экспортному контролю http://fstec.ru
11. Официальный сайт Федеральной службы безопасности http://fsb.ru
12. Официальный сайт Центрального банка РФ http://cbr.ru

Перечень информационных технологий
и программного обеспечения

1. Microsoft Word
2. Microsoft Excel
3. Microsoft PowerPoint
4. Microsoft Publisher
5. КонсультантПлюс / Гарант
6. Microsoft Internet Explorer/ Mozilla Firefox/ Opera

V. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Описание последовательности действий обучающихся (алгоритм изучения дисциплины)

Начиная изучение дисциплины «Кибербезопасность», студенту необходимо:

- ознакомиться с программой, изучить список рекомендуемой литературы; к программе курса необходимо будет возвращаться постоянно, по мере усвоения каждой темы в отдельности, для того чтобы понять: достаточно ли полно изучены все вопросы;
- внимательно разобраться в структуре дисциплины «Кибербезопасность», в системе распределения учебного материала по видам

занятий, формам контроля, чтобы иметь представление о практической части всего курса изучения;

- обратиться к электронным источникам, согласно учебному курсу по дисциплине «Кибербезопасность», позволяющим ориентироваться в последовательности выполнения заданий.

При подготовке к занятиям по дисциплине «Кибербезопасность» необходимо руководствоваться нормами времени на выполнение заданий. Например, при подготовке к занятию на проработку конспекта одной лекции, учебников, как правило, отводится от 0,5 часа до 2 часов, а на изучение первоисточников объемом 16 страниц печатного текста с составлением конспекта 1,5–2 часа, с составлением лишь плана около 1 часа.

Рекомендации по работе с литературой

Наиболее предпочтительна последовательность в работе с литературой. Ее можно представить в виде следующего примерного алгоритма:

- ознакомление с рабочей учебной программой и учебно-методическим комплексом дисциплины;
- изучение основной учебной литературы;
- проработка дополнительной (учебной и научной) литературы.

Для глубокого понимания сути темы, изложенной в рамках практического материала, рекомендуется затрачивать на прочтение основной и дополнительной литературы не менее 2 часов в неделю. В качестве поощрения студенты могут получать дополнительные баллы по самостоятельной работе с литературой: поиск литературы по заданной теме, сравнительный анализ научных публикаций, подготовка доклада и участие в научных конференциях. Основная литература подлежит обязательному изучению. Для подготовки к занятиям, текущей и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ДВФУ, расположенной по адресу http://www.dvfu.ru/library/electronic-resources/, где они имеют возможность получить доступ к учебно-методическим материалам, как библиотеки вуза, так и иных электронных библиотечных

систем. В свою очередь студенты могут взять необходимую литературу на абонементе вузовской библиотеки, а также воспользоваться читальными залами вуза.

В ходе чтения очень полезно, хотя и не обязательно, делать краткие конспекты прочитанного, выписки, заметки, выделять неясные, сложные для восприятия вопросы. В целях прояснения последних нужно обращаться к преподавателю. По завершении изучения рекомендуемой литературы полезно проверить уровень своих знаний с помощью контрольных вопросов для самопроверки.

Настоятельно рекомендуется избегать механического заучивания учебного материала. Практика убедительно показывает: самым эффективным способом является не «зубрежка», а глубокое, творческое, самостоятельное проникновение в существо изучаемых вопросов.

Необходимо вести систематическую каждодневную работу над литературными источниками. Объем информации по курсу настолько обширен, что им не удается овладеть в «последние дни» перед сессией, как на это иногда рассчитывают некоторые студенты.

Следует воспитывать в себе установку на прочность, долговременность усвоения знаний по курсу. Надо помнить, что они потребуются не только и не столько в ходе курсового зачета, но – что особенно важно – в последующей профессиональной деятельности.

Литература имеется в библиотеке университета.

Студент обязан знать не только рекомендуемую литературу, но и новые, существенно важные издания по курсу, вышедшие в свет после его публикации.

Рекомендации по подготовке для сдачи зачета согласно рейтинговой системе ДВФУ к зачету

Реализация дисциплины «Кибербезопасность» предусматривает

следующие виды учебной работы: практические занятия, самостоятельную работу студентов, текущий контроль и промежуточную аттестацию.

Освоение курса дисциплины «Кибербезопасность» предполагает рейтинговую систему оценки знаний студентов и предусматривает со стороны преподавателя текущий контроль за посещением студентами практических занятий, подготовкой и выполнением всех видов самостоятельной работы.

Промежуточной аттестацией по дисциплине «Кибербезопасность» является зачет, который проводится в виде устного опроса по вопросам.

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 «Кибербезопасность» при условии выполнения всех видов текущего контроля и самостоятельной работы, предусмотренных учебной программой.

Критерии оценки по дисциплине «Кибербезопасность» 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

Планирование – важнейшая черта человеческой деятельности, один из характерных, обязательных признаков человеческого труда. Для организации сложной учебной деятельности очень эффективным является использование средств, напоминающих о стоящих перед нами задачах, их последовательности выполнения. Такими средствами могут быть мобильный телефон, имеющий программу органайзера, включающего будильник, календарь и список дел; таймеры, напоминающие о выполнении заданий по дисциплине; компьютерные программы составления списка дел, выделяющие срочные и важные дела.

Составление списка дел – первый шаг к организации времени. Список имеет то преимущество, что позволяет видеть всю картину в целом. Упорядочение, классификация дел в списке – второй шаг к организации времени.

Регулярность – первое условие поисков более эффективных способов работы. Рекомендуется выбрать один день недели для регулярной подготовки по дисциплине. Регулярность не просто позволяет подготовиться к делу, она создает настрой на это дело, позволяет выработать правила выполнения дела (например, сначала проработка материала практических

занятий, учебника, чтение первоисточника, затем выделение и фиксирование основных идей в тетради).

Чтобы облегчить выполнение заданий, необходимо определить временные рамки. Еженедельная подготовка по дисциплине «Кибербезопасность» требует временных затрат. Четкое фиксирование по времени регулярных дел, закрепление за ними одних и тех же часов – важный шаг к организации времени. При учете времени надо помнить об основной цели рационализации – получить наибольший эффект с наименьшими затратами. Учет – лишь средство для решения основной задачи: сэкономить время.

Написание конспекта практических занятий: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на семинарском занятии

Для подготовки к практическому занятию необходима Проработка рабочей программы, уделяя особое внимание целям и задачам структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом практических занятий, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом.

Важная роль в организации учебной деятельности отводится программе дисциплины, дающая представление не только о тематической последовательности изучения курса, но и о затратах времени, отводимом на изучение курса. Успешность освоения дисциплины во многом зависит от правильно спланированного времени при самостоятельной подготовке (в зависимости от специальности от 2 – 3 до 5 часов в неделю).

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения лекционных занятий необходима аудитория, оснащенная мультимедийным проектором.

Для проведения практических занятий - аудитория, оснащенная мультимедийным проектором, персональными компьютерами на рабочих местах студентов с выходом в Интернет и установленным программным обеспечением (как минимум – Microsoft Office, Консультант Плюс / Гарант).

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 «Кибербезопасность»
38.04.02 «Менеджмент»
International Business and Project Management / Международный бизнес и управление проектами (на английском языке)

Форма подготовки: очная

Владивосток
2018

I. План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата / сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1.	В течение семестра	Выполнение практических заданий	36	Проверка наличия дополнительных материалов, файлов, выполнение заданий и их защита
2.	В течение семестра	Подготовка группового доклада	18	Проверка наличия материала практических занятий, файлов, выполнение заданий и их защита, активное участие в обсуждении вопросов по темам докладов.
ИТОГО			54	

II. Характеристика заданий для самостоятельной работы обучающихся, методические рекомендации по их выполнению

Рекомендации по самостоятельной работе студентов

Особое значение для освоения теоретического материала и для приобретения и формирования умений и навыков имеет самостоятельная работа студентов.

Самостоятельная работа студентов по дисциплине «Кибербезопасность» предусматривает изучение рекомендуемой основной и дополнительной литературы, решение практических заданий, подготовку к выполнению и защите групповых докладов и промежуточной аттестации – зачету.

Задание 1. Практические задачи. Темы для написания эссе. (Примеры)

1. Вы общаетесь в социальной сети со своими друзьями, и вам приходит сообщение от незнакомого человека: «Привет, классные фото! Только у меня все равно круче! Жми сюда!». Предлагается перейти по ссылке для просмотра фотографий. Как поступить в данной ситуации?

2. Вы находитесь в сети Интернет, изучаешь сайты с информацией о далеких планетах. Видите сайт, который предлагает составить твой гороскоп на год (месяц, неделю). Заходите на сайт, отвечаете на все предложенные вопросы. В конце опроса вам предлагается ввести номер мобильного телефона. Какими будут ваши действия? Почему?

3. Вам позвонил друг и сообщил, что увидел в сети Интернет сообщение о срочном сборе средств для больного ребенка. Деньги предлагается перевести на счет указанного мобильного телефона или на электронный кошелек. Вам друг настаивает на помощи ребенку. Какими должны быть ваши действия? Почему?

4. Во время общения в социальной сети вам приходит сообщение: «Привет! Я твой ровесник, посмотрел страничку, мне все понравилось. Хочу с тобой дружить. Давай сходим в кино?» Что вы будете делать в этой ситуации? Почему?

Темы для написания эссе.

1. Построение систем обеспечения информационной безопасности на предприятии.
2. Обеспечение информационной безопасности бизнеса.
3. Система управления информационной безопасностью бизнеса.
4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.
5. Социальные аспекты системы управления информационной безопасностью бизнеса.
6. Управление жизненным циклом информационных активов. Анализ влияния состояния информационных активов на деятельность организации.
7. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
8. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.
9. Подходы к формированию нормативного обеспечения системы информационной безопасности организации.
10. Аудит методов и средств обеспечения информационной безопасности организации.

11. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.
12. Организация системы управления информационной безопасностью как социальная система.
13. Организационные основы и принципы деятельности службы защиты информации на предприятии.
14. Структура службы защиты информации на предприятии.
15. Бюджет и штат службы защиты информации на предприятии.
16. Подбор и расстановка сотрудников службы защиты информации на предприятии.
17. Подготовка сотрудников службы защиты информации на предприятии.
18. Организация труда сотрудников подразделения защиты сетей.
19. Организация труда сотрудников подразделения мониторинга информационной безопасности.
20. Сущность, организация и принципы управления службой защиты информации на предприятии.
21. Методы и технологии управления службой защиты информации на предприятии.

Качественные критерии оценки эссе:

- знание и понимание проблемы;
- умение систематизировать и анализировать материал, четко и обоснованно формулировать выводы;
- «трудозатратность» (объем изученной литературы, добросовестное отношение к анализу проблемы);
- самостоятельность, способность к определению собственной позиции по проблеме и к практической адаптации материала, недопустимость (!) плагиата;
- выполнение необходимых формальностей (точность в цитировании и указании источника текстового фрагмента, аккуратность оформления)

Критерии оценки:

- 100-86 баллов выставляется студенту, если студент выразил свое мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные нормативных и технических документов. Студент знает и владеет навыком самостоятельной работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно;

- 85-76 баллов – работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные нормативных и технических документов. Продемонстрированы практические умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы;

- 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены нормативные и технические документы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы;

60-50 баллов – если работа представляет собой полностью переписанный исходный текст, без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Темы и ориентировочное содержание аналитических, научно-исследовательских и творческих заданий

Задание 2. На основании изучения литературы, рекомендованной преподавателем, подготовить групповой доклад на одну из тем и представить презентацию на выбранную тему.

Методические указания для выполнения самостоятельной работы по заданию 2: «Доклад на выбранную тему».

Темы для раскрытия в первой части домашнего задания.

1. Основные понятия в области кибербезопасности Интернета вещей в менеджменте;
2. Основные угрозы, риски и уязвимости в сфере кибербезопасности Интернета вещей и критической информационной инфраструктуры в международном бизнесе;
3. Основные протоколы передачи данных и аутентификации, используемые в «Интернет вещей»;
4. Основные понятия в сфере функциональной безопасности в рамках менеджмента;
5. Положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
6. Положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности экономических объектов;
7. Основные средства обеспечения кибербезопасности (архитектура, принципы построения) в системе управления;
8. Принципы проектирования систем безопасности значимых объектов на примере международных компаний;
9. Состав и способы организации деятельности сил обеспечения кибербезопасности объектов;
10. Основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры в проектной деятельности на международном рынке;

11. Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан;

12. Классификация и примеры продуктов «Интернет-вещей» международных компаний - примеры угроз, уязвимостей, рисков;

13. Основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере международного менеджмента;

14. Основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей;

15. Примеры юридических инцидентов в области регулирования кибербезопасности «Интернета-вещей» на международном рынке.

Используя учебную литературу, научные публикации и интернет-ресурсы, осуществить поиск информации по выбранной тематике. Изучить теоретические материалы, мнение экспертов.

Обсудить в своей группе отобранные материалы по выбранной тематике, коллективно разработать план ее изложения перед студенческой аудиторией. Распределить в группе задания, обязанности по доработке темы в соответствие с разработанным планом (например, осуществить поиск недостающих фактических данных, нормативно-законодательных актов, примеров).

Подготовить презентацию и файл в процессоре MS Word с сопроводительным текстом к каждому слайду.

Осуществить поиск правовых документов по теме в справочно-правовой системе Консультант Плюс, сформировать папку с отобранными нормативно-законодательными актами, подготовить закладки на нужные фрагменты текста в документах.

Рекомендации по работе с литературой

При самостоятельной работе с рекомендуемой литературой студентам необходимо придерживаться определенной последовательности:

- при выборе литературного источника теоретического материала

лучше всего исходить из основных понятий изучаемой темы курса, чтобы точно знать, что конкретно искать в том или ином издании;

- для более глубокого усвоения и понимания материала следует читать не только имеющиеся в тексте определения и понятия, но и конкретные примеры;
- чтобы получить более объемные и системные представления по рассматриваемой теме необходимо просмотреть несколько литературных источников (возможно альтернативных);
- не следует конспектировать весь текст по рассматриваемой теме, так как такой подход не дает возможности осознать материал; необходимо выделить и законспектировать только основные положения, определения и понятия, позволяющие выстроить логику ответа на изучаемые вопросы.

Методические рекомендации по подготовке презентации

1. Первый слайд должен содержать название доклада, ФИО и координаты (номер группы, направление подготовки, адрес электронной почты) выступающего. Каждый слайд должен иметь заголовок.

2. Презентация начинается с аннотации, где на одном-двух слайдах дается представление, о чем пойдет речь. Большая часть презентаций требует оглашения структуры.

3. Переход от слайда к сладу организуйте по щелчку мыши. Оптимальная скорость переключения – один слайд за 1–2 минуты. Слушатели должны успеть воспринять информацию и визуально со слайда, и на слух. «Универсальная» оценка – число слайдов равно продолжительности выступления в минутах.

4. Размер шрифта основного текста – не менее 16pt, заголовки ≥ 20 pt. Наиболее читабельным и традиционно используемым в научных исследованиях является Times New Roman. Оформляйте все слайды в едином стиле.

5. Презентация является дополнением к докладу. Каждый слайд – «плакат», поэтому должен содержать таблицы с фактическими данными и диаграммы (с обязательным указанием ссылок на источники в случае, если они подготовлены несамостоятельно), информацию в виде схем и рисунков. Сопроводительный текст к каждому слайду сохраните либо в разделе Заметки, либо в файле MS Word.

6. Не перегружайте слайд информацией. Не делайте много мелкого текста. При подготовке презентации рекомендуется в максимальной степени использовать графики, схемы, диаграммы и модели с их кратким описанием. Фотографии и рисунки делают представляемую информацию более интересной и помогают удерживать внимание аудитории, давая возможность ясно понять суть предмета. Длинные перечисления или большие таблицы с числами тяжело воспринимаются, лучше построить графики.

7. Имеет смысл быть аккуратным. Неряшливо сделанные слайды (разнобой в шрифтах и отступах, ошибки и опечатки) вызывают подозрение, что и к содержательным вопросам докладчик подошёл «спустя рукава». Готовую презентацию надо просмотреть внимательно несколько раз «свежим» взглядом для выявления проблем с оформлением и опечаток.

8. Если Вы чувствуете себя хоть немного неуверенно перед аудиторией, или выступление очень ответственное, то напишите и выучите свою речь наизусть. Озвучивание одной страницы (формат А4, шрифт 14pt, полуторный интервал) занимает 2 минуты. Потренируйтесь выступать с вашей презентацией. Пусть кто-то послушает и скажет Ваши ошибки, впечатление о выступлении, что интересно, что непонятно, как Вы выглядели.

9. Следите за временем (регламент выступления – 10-15 минут).

10. Речь и слайды не должны совпадать, тогда презентация станет «объёмной». Стиль речи должен быть понятным для аудитории, используйте примеры, ассоциации и образы. Слайды могут содержать больше

«технических» подробностей: формулы, схемы, таблицы, графики. Всегда подписывайте оси (какая переменная и ее размерность).

11. Первые же фразы должны интриговать. Например, можно сказать о том, насколько сложной или насколько важной является данная задача, или о том, насколько неожиданным будет решение – это позволит удержать внимание слушателей до конца. Но тогда концовка действительно должна оказаться нетривиальной – иначе слушатель будет разочарован. Запомните, у Вас только 20 секунд в начале доклада для того, чтобы привлечь внимание слушателей. Если за это время не прозвучит нечто поистине интригующее (или хотя бы хорошая шутка), вернуть внимание будет очень сложно.

12. Люди лучше запоминают то, что увидели последним!

13. В серьёзных научных презентациях не следует использовать эффекты анимации и излишнее «украшательство».

14. Заранее продумайте возможные проблемы с техникой. Заранее скопируйте на рабочий стол файл с презентацией и проверьте, как он работает, с первого до последнего слайда. Обязательно имейте при себе копию презентации на флэш-карте. Проверьте, нет ли проблем с отображением русских шрифтов и формул.

Критерии оценки выполнения коллективного научно-исследовательского, творческого задания

№ п/п	Критерий	Количество баллов
1	Готовность результатов самостоятельной работы в срок	10
2	Доклад с демонстрацией презентации, ответы на вопросы аудитории	20
3	Материал современный, актуальный, интересный для аудитории	25
4	Тема раскрыта глубоко, изложение материала логично, аргументированно, подкреплено иллюстрациями, таблицами и диаграммами с фактическими данными, схемами и рисунками	25
5	Наличие папки с нормативно-законодательными актами, закладками в СПС Консультант Плюс, презентации и файла MS Word с текстовым материалом	20
	ИТОГО	100

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 «Кибербезопасность»
Специальность 38.04.02 «Менеджмент»
International Business and Project Management / Международный бизнес и управление проектами (на английском языке)
Форма подготовки: очная

Владивосток
2018

Паспорт
фонда оценочных средств
по дисциплине «Кибербезопасность»

Код и формулировка компетенции	Этапы формирования компетенции	
ПК-3 – способность использовать современные методы управления корпоративными финансами для решения стратегических задач;	знает	Знает: сущность решений защиты информации кибернетических систем; основы оценивания влияния средств защиты информации на критически важные экономические объекты информатизации.
	умеет	Умеет: находить решения стандартных задач профессиональной деятельности на основе методов оптимизации систем защиты информации и управления корпоративными финансами для решения стратегических задач.
	владеет	Владеет: способность формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.
ПК-9 владением методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде	знает	Знает: сущность методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.
	умеет	Умеет:формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.
	владеет	Владеет: способность оценивать влияние средств защиты информации на критически важные экономические объекты информатизации.

Контроль достижений целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в проблему кибербезопасности - Раздел II. Особенности защиты кибернетических систем	ПК-3	Знает: сущность решений защиты информации кибернетических систем; основы оценивания влияния средств защиты информации на критически важные экономические объекты информатизации	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету1-15.
			Умеет: находить решения стандартных задач профессиональной деятельности на основе	решение практических заданий; ситуационные задачи (ПР-11);	Вопросы к зачету1-15.

			методов оптимизации систем защиты информации и управления корпоративными финансами для решения стратегических задач	самостоятельная работа (Приложение 2)	
			Владеет: способностью формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету1-15.
2	Раздел II. Особенности защиты кибернетических систем - Раздел III. Технологии угроз сетевой безопасности	ПК-9	Знает: сущность методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету1-15.
			Умеет: формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету1-15.
			Владеет: способность оценивать влияние средств защиты информации на критически важные экономические объекты информатизации.	решение практических заданий; ситуационные задачи (ПР-11); самостоятельная работа (Приложение 2)	Вопросы к зачету1-15.

Оценочные средства для проверки сформированности компетенций

Код и формулировка компетенции	Задание
ПК-3 – способность использовать современные методы управления корпоративными финансами для решения стратегических задач	Ситуация: Вы рассматриваете решение о приобретении акций молодой авиакомпании. Размер дивидендов сильно изменялся из года в год. Однако компания четко выдерживает долю выплаты дивидендов на уровне 40 %. Финансовая отчетность показывает, что в прошлом году чистая при- быль компании составила 2 млрд дол. Аналитики говорят, что темп роста чистой прибыли в первый год составит 7 %, во второй – 10 %, а в третий – 8 %. После этого все ожидают наступления стабилизации и прогнозируют рост финансовых показателей на уровне 3 %. Ожидают также, что после вступления в стабильную фазу менеджеры авиакомпании примут решение уменьшить долю чистой прибыли, направляемой на инвестиции, до 30 %. Требуемая доходность инвестиций в акции этой компании составляет 10 %. Количество акций, обращающихся на рынке, составляет 250 млн шт. Определите подлинную стоимость одной акции авиакомпании. Какова ваша стратегия?

ПК-9 владением методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде	Задание 1. Предположим, что домохозяйства решили по каким-то причинам сберегать более высокую долю своих доходов при любом их уровне. В результате функция потребления из C1 = $0,5 \cdot Y$ превратилась в C2 = $0,2 \cdot Y$. Инвестиции в обоих случаях составляют 200 млрд руб. 1. Какое воздействие па уровень доходов оказало изменение функции потребления? Каким будет новый уровень равновесных доходов? 2. Сберегают ли домохозяйства более высокую долю своих доходов в условиях нового равновесия? 3. Сберегают ли домохозяйства в условиях нового равновесия абсолютно больше, чем ранее? Задание 2.Первоначально экономика находится в состоянии долгосрочного равновесия и описывается следующим образом: долгосрочная кривая AS вертикальна на уровне Y = 2800, краткосрочная кривая AS горизонтальна на уровне P = 1,0, кривая AD задана уравнением $Y = 3,5 \cdot \frac{M}{P}$, где M = 800. Произошел неблагоприятный шок предложения, в результате чего цены выросли до уровня 1,4 (SRAS'), а потенциальный уровень выпуска снизился до уровня Y = 2500 (LRAS'). а) каковы новые равновесные значения Y и P в краткосрочном и долгосрочном периодах, если правительство и Центральный банк не вмешиваются в экономику, т.е. кривая AD остается прежней? б) если Центральный банк проведет стабилизационную политику, то какое дополнительное количество денег он должен выпустить в обращение, чтобы краткосрочное равновесие в экономике установилось на уровне выпуска Y = 2800? в) если возросшее количество денег в экономике будет поддерживаться и далее, то каковы будут координаты точки нового долгосрочного равновесия?

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**Критерии**	**Показатели**
ПК-3 – способность использовать современные методы управления корпоративным и финансами для решения стратегических задач	знает (порого-вый уровень)	Знает: сущность решений защиты информации кибернетических систем; основы оценивания влияния средств защиты информации на критически важные экономические объекты информатизации	знание правовых, нормативных и (законодательные и нормативные акты РФ, и др.), необходимых для осуществления финансовой деятельностью	- способность перечислить и охарактеризовать правовые акты, регламентирующие финансовую деятельность; - способность грамотно интерпретировать показатели финансовой отчетности предприятия -
	умеет (продви-нутый)	Умеет: находить решения стандартных задач	знает основные финансовые показатели для	- способность проводить расчеты финансовых показателей, составлять

		профессиональной деятельности на основе методов оптимизации систем защиты информации и управления корпоративными финансами для решения стратегических задач	расчета бизнес-планов и критерии деловой и инвестиционной привлекательности	финансовую, управленческую отчетность и финансовые отчеты с прогнозированием и построением ожиданий
	владеет (высокий)	Владеет: способностью формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде	владеет основными критериями эффективности проектами	- способность принимать эффективные управленческие решения на основе полученной финансовой информации
ПК-9 - владение методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде	знает (поро-говый уровень)	сущность методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.	знание правовых, нормативных и (законодательные и нормативные акты РФ, и др.), необходимых для составления бухгалтерской, управленческой и налоговой отчетности	- способность характеризовать полученную информацию на основании нормативных и законодательных актов
	умеет (продви-нутый)	формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.	знает основные показатели в управленческой, налоговой и финансовой отчетности	- умеет грамотно интерпретировать показатели отчетности и проводить расчеты согласно бухгалтерским стандартам
	владеет (высокий)	способность оценивать влияние средств защиты информации на критически важные экономические объекты информатизации.	владеет основыными навыками финансового моделирования и прогнозирования	- способность построения финансовых моделей предприятия, расчета затрат и разработки предложений для компаний

Зачетно-экзаменационные материалы

Оценочные средства для промежуточной аттестации

Вопросы к зачету

1. Основные понятия в области кибербезопасности Интернета вещей в менеджменте;
2. Основные угрозы, риски и уязвимости в сфере кибербезопасности Интернета вещей и критической информационной инфраструктуры в международном бизнесе;
3. Основные протоколы передачи данных и аутентификации, используемые в «Интернет вещей»;
4. Основные понятия в сфере функциональной безопасности в рамках менеджмента;
5. Положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
6. Положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности экономических объектов;
7. Основные средства обеспечения кибербезопасности (архитектура, принципы построения) в системе управления;
8. Принципы проектирования систем безопасности значимых объектов на примере международных компаний;
9. Состав и способы организации деятельности сил обеспечения кибербезопасности объектов;
10. Основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры в проектной деятельности на международном рынке;
11. Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан;
12. Классификация и примеры продуктов «Интернет-вещей» международных компаний - примеры угроз, уязвимостей, рисков;

13. Основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере международного менеджмента;

14. Основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей;

15. Примеры юридических инцидентов в области регулирования кибербезопасности «Интернета-вещей» на международном рынке.

Критерии оценки студента на зачете по дисциплине «Кибербезопасность»

Баллы (рейтинговой оценки)	**Оценка зачета/ 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 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

Тематика практических занятий

по дисциплине «Кибербезопасность»

Практическое занятие 1-2-3. Введение в проблему кибербезопасности. Введение в теорию доверенных систем (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (2 час.)

- Понятие кибербезопасности.
- Роль человека в кибернетических системах
- Проблема информационной безопасности в кибернетических системах
- Понятие доверенной информационной системы
- Отношения доверия в информационных системах
- Решение кейсов

Практическое занятие 4-5-6-8. Понятие критически важного объекта. Основы правового регулирования защиты информации критически важных объектов и современные методы управления корпоративными финансами для решения стратегических задач (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (4 час.)

- Понятие критически важного объекта
- Особенности функционирования критически важных объектов
- Требования к информационной безопасности критически важных экономических объектов
- Основы правового регулирования вопросов защиты информации на критически важных экономических объектах
- Решение кейсов

Практическое занятие 9-10-11. Особенности защиты кибернетических систем: Internet- вещей, smart things (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (6 час.)

- Кибернетические системы, характеристики, жизненный цикл, проблема сопровождения больших кибернетических систем в рамках поведения экономических агентов и рынков в глобальной среде
- Особенности эксплуатации, ограничения, связанные с длительными сроками эксплуатации систем Internet вещей, smart things – коммуникация и принятие решений без участия человека
- Требования к обеспечению безопасности управления корпоративными финансами для решения стратегических задач
- Решение кейсов

Практическое занятие 12-13. Требования к системам защиты информации при интеграции с системами реального времени и методы экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде (8 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (4 час.)

- Определение систем реального времени с точки зрения информационной безопасности управления корпоративными финансами для решения стратегических задач
- Определение требований к обеспечению информационной безопасности экономических агентов и рынков в глобальной среде
- Решение кейсов

Практическое занятие 14-15. Методологические рекомендации по анализу режимов работы. Кибернетических систем управления корпоративными финансами для решения стратегических задач (4 час.)

Метод активного / интерактивного обучения – метод ситуационного анализа (ситуационные задачи/кейс-стади) (2 час.)

- Степень влияния на систему в целом. Зависимость опасности выявленных уязвимостей от качества управления корпоративными финансами для решения стратегических задач
- Виды идентификации, применяемые в современных экономических условиях
- Понятие идентификационной сущности экономических агентов и рынков в глобальной среде
- Проблема хранения идентификационной сущности
- Процедуры идентификации без участия человека
- Решение кейсов

Критерии оценки:

- 100-86 баллов выставляется студенту, если студент выразил свое мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные нормативных и технических документов. Студент знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно;

- 85-76 баллов – работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные нормативных и технических документов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы;

- 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены

нормативные и технические документы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы;

- 60-50 баллов – если работа представляет собой полностью переписанный исходный текст, без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Кейсы по дисциплине «Кибербезопасность» (примеры).

1. Кейс 1. 2017, The hacks that left us exposed in 2017 by Selena Larson December 20, 2017 (https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html)
2. Кейс 2. 5 huge cybersecurity breaches at companies you know by Benjamin Snyder, October 3, 2014 (http://fortune.com/2014/10/03/5-huge-cybersecurity-breaches-at-big-companies/)
3. Кейс 3. CYBERSECURITY: INDUSTRY REPORT & INVESTMENT CASEб By Gaurav Pendse / Product Development Specialist, Nasdaq Global Information Services (https://business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html)

Выберите 2 кейса (вы можете найти свой кейс) по кибербезопасности и проанализируйте следующие ее элементы:

- Год
- Исследуемый вопрос
- Гипотеза
- Методология изучения проблемы

Критерии оценки:

- 100-86 баллов выставляется студенту, если студент выразил свое мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные нормативных и технических документов. Студент знает и владеет навыком самостоятельной работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно;

- 85-76 баллов – работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные нормативных и технических документов. Продемонстрированы практические умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы;

- 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены нормативные и технические документы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы;

- 60-50 баллов – если работа представляет собой полностью переписанный исходный текст, без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Практические задачи. Темы для написания эссе. (Примеры)

1. Вы общаетесь в социальной сети со своими друзьями, и вам приходит сообщение от незнакомого человека: «Привет, классные фото! Только у меня

все равно круче! Жми сюда!». Предлагается перейти по ссылке для просмотра фотографий. Как поступить в данной ситуации?

2. Вы находитесь в сети Интернет, изучаешь сайты с информацией о далеких планетах. Видите сайт, который предлагает составить твой гороскоп на год (месяц, неделю). Заходите на сайт, отвечаете на все предложенные вопросы. В конце опроса вам предлагается ввести номер мобильного телефона. Какими будут ваши действия? Почему?

3. Вам позвонил друг и сообщил, что увидел в сети Интернет сообщение о срочном сборе средств для больного ребенка. Деньги предлагается перевести на счет указанного мобильного телефона или на электронный кошелек. Вам друг настаивает на помощи ребенку. Какими должны быть ваши действия? Почему?

4. Во время общения в социальной сети вам приходит сообщение: «Привет! Я твой ровесник, посмотрел страничку, мне все понравилось. Хочу с тобой дружить. Давай сходим в кино?» Что вы будете делать в этой ситуации? Почему?

Темы для написания эссе.

1. Построение систем обеспечения информационной безопасности на предприятии.
2. Обеспечение информационной безопасности бизнеса.
3. Система управления информационной безопасностью бизнеса.
4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.
5. Социальные аспекты системы управления информационной безопасностью бизнеса.
6. Управление жизненным циклом информационных активов. Анализ влияния состояния информационных активов на деятельность организации.
7. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
8. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.
9. Подходы к формированию нормативного обеспечения системы информационной безопасности организации.

10. Аудит методов и средств обеспечения информационной безопасности организации.

11. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.

12. Организация системы управления информационной безопасностью как социальная система.

13. Организационные основы и принципы деятельности службы защиты информации на предприятии.

14. Структура службы защиты информации на предприятии.

15. Бюджет и штат службы защиты информации на предприятии.

16. Подбор и расстановка сотрудников службы защиты информации на предприятии.

17. Подготовка сотрудников службы защиты информации на предприятии.

18. Организация труда сотрудников подразделения защиты сетей.

19. Организация труда сотрудников подразделения мониторинга информационной безопасности.

20. Сущность, организация и принципы управления службой защиты информации на предприятии.

21. Методы и технологии управления службой защиты информации на предприятии.

Качественные критерии оценки эссе:

- знание и понимание проблемы;
- умение систематизировать и анализировать материал, четко и обоснованно формулировать выводы;
- «трудозатратность» (объем изученной литературы, добросовестное отношение к анализу проблемы);
- самостоятельность, способность к определению собственной позиции по проблеме и к практической адаптации материала, недопустимость (!) плагиата;

• выполнение необходимых формальностей (точность в цитировании и указании источника текстового фрагмента, аккуратность оформления)

Критерии оценки:

- 100-86 баллов выставляется студенту, если студент выразил свое мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные нормативных и технических документов. Студент знает и владеет навыком самостоятельной работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно;

- 85-76 баллов – работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные нормативных и технических документов. Продемонстрированы практические умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы;

- 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены нормативные и технические документы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы;

60-50 баллов – если работа представляет собой полностью переписанный исходный текст, без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Тематика групповых докладов

по дисциплине «Кибербезопасность»

1. Основные понятия в области кибербезопасности Интернета вещей в менеджменте;
2. Основные угрозы, риски и уязвимости в сфере кибербезопасности Интернета вещей и критической информационной инфраструктуры в международном бизнесе;
3. Основные протоколы передачи данных и аутентификации, используемые в «Интернет вещей»;
4. Основные понятия в сфере функциональной безопасности в рамках менеджмента;
5. Положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
6. Положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности экономических объектов;
7. Основные средства обеспечения кибербезопасности (архитектура, принципы построения) в системе управления;
8. Принципы проектирования систем безопасности значимых объектов на примере международных компаний;
9. Состав и способы организации деятельности сил обеспечения кибербезопасности объектов;
10. Основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры в проектной деятельности на международном рынке;
11. Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан;
12. Классификация и примеры продуктов «Интернет-вещей» международных компаний - примеры угроз, уязвимостей, рисков;

13. Основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере международного менеджмента;

14. Основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей;

15. Примеры юридических инцидентов в области регулирования кибербезопасности «Интернета-вещей» на международном рынке.

Критерии оценки выполнения коллективного научно-исследовательского, творческого задания

№ п/п	Критерий	Количество баллов
1	Готовность результатов самостоятельной работы в срок	10
2	Доклад с демонстрацией презентации, ответы на вопросы аудитории	20
3	Материал современный, актуальный, интересный для аудитории	25
4	Тема раскрыта глубоко, изложение материала логично, аргументированно, подкреплено иллюстрациями, таблицами и диаграммами с фактическими данными, схемами и рисунками	25
5	Наличие папки с нормативно-законодательными актами, закладками в СПС Консультант Плюс, презентации и файла MS Word с текстовым материалом	20
	ИТОГО	100

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

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

Текущая аттестация по дисциплине «Кибербезопасность» проводится в форме контрольных мероприятий (выполнение заданий на практических занятиях, решение ситуационных задач, написание групповых докладов) 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 практических занятий, 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 решения заданий);

- результаты самостоятельной работы (задания и критерии оценки размещены в Приложении 1).

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

Итоговый контроль. Предусматривает рейтинговую оценку по учебной дисциплине в течении семестра в процессе обучения.

Краткая характеристика процедуры применения используемого оценочного средства. В результате посещения практических занятий, семинаров и круглых столов студент последовательно осваивает материалы дисциплины и изучает ответы на вопросы к зачету, представленные в структурном элементе ФОС IV.1. В ходе промежуточной аттестации студент готовит индивидуальное творческое зачетное задание (индивидуальное творческое зачетное задание размещено в структурном элементе ФОС IV.2). Критерии оценки студента на зачете представлены в структурном элементе ФОС IV.3. Критерии оценки текущей аттестации – контрольная проверка знаний (практические занятия, групповое творческое задание) представлены в структурном элементе ФОС V.

Критерии выставления оценки студенту на зачете

по дисциплине «Кибербезопасность»

Баллы (рейтинговой оценки)	**Оценка зачета** (стандартная)	**Требования к сформированным компетенциям**
86-100	«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.
85-76	«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	«удовлетвори-тельно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
60-0	«неудовлетвори-тельно»	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.