Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Рабочая программа дисциплины
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БИЗНЕСА

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.07.04.02**
Трудоемкость в зачетных единицах:	**8 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**8 семестр - 16 часов;**
Практические занятия	**8 семестр - 16 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**8 семестр - 2 часа;**
Самостоятельная работа	**8 семестр - 145,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Контрольная работа**	
Промежуточная аттестация:	
Экзамен	**8 семестр - 0,5 часа;**

Москва 2018

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Горбенко А.О. Идентификатор: R687e85ac-GorbenkoAO-2a54ef20	А.О. Горбенко
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Освоение обучающимися профессиональных компетенций, заключающихся в общей готовности и способности применять на практике предлагаемые в настоящее время методы защиты конфиденциальной информации (правовые, организационные, программные и аппаратные) при организации и поддержке электронного бизнеса

Задачи дисциплины

- получения теоретических знаний в области применения защитных механизмов при организации и ведении электронного бизнеса;
- получения практических навыков в области применения защитных механизмов при организации и ведении электронного бизнеса.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты		знать: - методы защиты конфиденциальной информации (правовые, организационные, программные и аппаратные) при организации и поддержке электронного бизнеса. уметь: - администрировать подсистемы информационной безопасности объекта защиты.
ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации		уметь: - организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности организации; - применять навыки в области применения защитных механизмов при организации и ведении электронного бизнеса.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Основные модели электронной коммерции	18	8	4	-	4	-	-	-	-	-	10	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основные модели электронной коммерции"
1.1	Тема 1. Введение в дисциплину	18		4	-	4	-	-	-	-	-	10	-	
2	Угрозы безопасности электронной коммерции и электронных платежей. Безопасность банковских структур	38		4	-	4	-	-	-	-	-	30	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Угрозы безопасности электронной коммерции и электронных платежей. Безопасность банковских структур" подготовка к выполнению заданий на практических занятиях
2.1	Потенциальные угрозы электронного бизнеса	12		1	-	1	-	-	-	-	-	10	-	
2.2	Построение модели злоумышленника	12		1	-	1	-	-	-	-	-	10	-	
2.3	Классификация преступлений в электронном бизнесе	14		2	-	2	-	-	-	-	-	10	-	
3	Методы и средства обеспечения информационной безопасности электронного бизнеса	50		4	-	4	-	-	-	-	-	42	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Методы и средства обеспечения информационной безопасности электронного бизнеса" подготовка к выполнению заданий на практических занятиях ***Изучение материалов литературных источников:***
3.1	Правовые основы обеспечения информационной	12		1	-	1	-	-	-	-	-	10	-	

	безопасности													[4], 5-8
3.2	Методы контроля и разграничения доступа к информации	12		1	-	1	-	-	-	-	-	10	-	[6], 15-65
3.3	Использование механизмов и средств криптографической защиты информации в системах электронного бизнеса	12		1	-	1	-	-	-	-	-	10	-	
3.4	Основы безопасности электронной торговли при использовании пластиковых карт. К	14		1	-	1	-	-	-	-	-	12	-	
4	Политика информационной безопасности. Построение систем безопасности электронного бизнеса	38		4	-	4	-	-	-	-	-	30	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Политика информационной безопасности. Построение систем безопасности электронного бизнеса" подготовка к выполнению заданий на практических занятиях
4.1	Политика информационной безопасности в системах электронной коммерции	14		2	-	2	-	-	-	-	-	10	-	***Изучение материалов литературных источников:*** [1], 67-95 [2], 57-95 [3], 32-90 [5], 25-100
4.2	Стандарт Центрального банка России по защите информации (СТО БР ИББС-1.0–2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (с изменениями 2010 и	12		1	-	1	-	-	-	-	-	10	-	

	2014 г.)													
4.3	Основы построения и менеджмента систем безопасности электронного бизнеса. Аудит систем информационной безопасности электронного бизнеса	12		1	-	1	-	-	-	-	-	10	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**16**	**-**	**16**	**-**	**2**	**-**	**-**	**0.5**	**112**	**33.5**	
	Итого за семестр	**180.0**		**16**	**-**	**16**	**2**		**-**		**0.5**	**145.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Основные модели электронной коммерции

1.1. Тема 1. Введение в дисциплину

Основные понятия и термины электронной коммерции и бизнеса. Понятие электронной коммерции. Краткий обзор основных понятий. Типология электронной коммерции.

2. Угрозы безопасности электронной коммерции и электронных платежей. Безопасность банковских структур

2.1. Потенциальные угрозы электронного бизнеса

Основные задачи обеспечения безопасности информации хозяйствующего субъекта при ведении электронного бизнеса.

2.2. Построение модели злоумышленника

Цель злоумышленника, пути проникновения, средства атаки, подготовка и должность.

2.3. Классификация преступлений в электронном бизнесе

Классификация и общая характеристика компьютерных преступлений. Анализ и оценка последствий компьютерных преступлений на основе современной статистики.

3. Методы и средства обеспечения информационной безопасности электронного бизнеса

3.1. Правовые основы обеспечения информационной безопасности

Законодательство и нормативно-правовое регулирование в сфере информационной безопасности. Проблемы обеспечения безопасности электронного бизнеса при работе в Internet. Методы и средства защиты информации при работе в Interne.

3.2. Методы контроля и разграничения доступа к информации

Идентификация и аутентификация. Электронные ключи. Биометрические методы и средства. Применение брандмауэров для защиты информации в системах электронного бизнеса.

3.3. Использование механизмов и средств криптографической защиты информации в системах электронного бизнеса

Криптографическая аутентификация. Схемы аутентификации на основе симметричных ключей. Электронная цифровая подпись. Хеширование . Криптографические алгоритмы.

3.4. Основы безопасности электронной торговли при использовании пластиковых карт. К

Классификация пластиковых карт. Обеспечение безопасности банковских терминалов. Защищенные протоколы (SSL, SET). Методы защиты информации в наиболее известных платежных системах.

4. Политика информационной безопасности. Построение систем безопасности электронного бизнеса

4.1. Политика информационной безопасности в системах электронной коммерции

Стандарты построения систем защиты информации и практическое применение их требований для обеспечения информационной безопасности систем электронной коммерции. Корпоративные стандарты обеспечения информационной безопасности систем.

4.2. Стандарт Центрального банка России по защите информации (СТО БР ИББС-1.0–2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (с изменениями 2010 и 2014 г.)

Обеспечение безопасности в банковской сфере. Электронные платежные системы. Классификация и особенности применения в РФ. Основные принципы внедрения платежных систем в электронную коммерцию. Система организационно-распорядительных документов организации по вопросам обеспечения безопасности информационных технологий.

4.3. Основы построения и менеджмента систем безопасности электронного бизнеса. Аудит систем информационной безопасности электронного бизнеса

Состав и организационная структура системы обеспечения информационной безопасности. Распределение функций и порядок взаимодействия подразделений на различных этапах жизненного цикла информационных подсистем. Ответственные за информационную безопасность в подразделениях.

3.3. Темы практических занятий

1. 13. Основные защитные механизмы: фильтрация пакетов, трансляция сетевых адресов, промежуточная аутентификация, проверка почты, виртуальные частные сети, противодействия атакам, нацеленным на нарушение работоспособности сетевых служб, дополнительные функции (1 час).;
2. 12.Межсетевые экраны. Назначение и виды. Основные возможности и варианты размещения. Достоинства и недостатки (1 час).;
3. 11.Способы устранения уязвимостей и противодействия вторжениям нарушителей (1 час).;
4. 10.Проблемы обеспечения безопасности в сетях. Сетевые угрозы, уязвимости и атаки. Средства обнаружения уязвимостей узлов IP-сетей и атак на узлы, протоколы и сетевые службы. Получение оперативной информации о новых уязвимостях и атаках(1 час).;
5. 9.Задачи, решаемые средствами защиты информации от несанкционированного доступа. Требования руководящих документов ФСТЭК (Гостехкомиссии) России к средствам защиты информации от несанкционированного доступа (1 час).;
6. 8. Обзор и методы использования платежных систем. Обработка кредитных карт и цифровой наличности. Пластиковые карты их классификация. Применения в системах электронного бизнеса (1 час).;
7. 2.Угрозы информационной безопасности и их классификация. Основные источники и пути реализации угроз. Модели нарушителей. Подходы к анализу и управлению рисками, к категорированию ресурсов и определению требований к уровню обеспечения информационной безопасности. Российские, зарубежные (британский BS7799 - ISO 17799 и германский BSI) и международные стандарты и критерии защищенности систем (ISO15408-99) (1 час).;
8. 3.Основные защитные механизмы. Идентификация и аутентификация, разграничение доступа, регистрация и аудит, контроль целостности, криптографические механизмы обеспечения конфиденциальности, целостности и аутентичности информации, фильтрация пакетов, трансляция адресов, контроль вложений, обнаружение и противодействие атакам, сканирование уязвимостей и др (1 час).;
9. 5.Состав и организационная структура системы обеспечения информационной безопасности. Распределение функций и порядок взаимодействия подразделений на различных этапах жизненного цикла информационных подсистем. Ответственные за информационную безопасность в подразделениях. Администраторы штатных и дополнительных средств защиты. Подразделения технической защиты информации (1 час).;

10. 4.Анализ законодательства РФ и других нормативно-правовых документов, регламентирующих отношения субъектов в информационной сфере и деятельность организаций по защите информации. Защита информации ограниченного доступа, обязанности и права субъектов. Лицензирование деятельности, сертификация средств защиты и аттестация информационных систем. Требования руководящих документов ФСТЭК (Гостехкомиссии) России и ФСБ (1 час).;
11. 15.Виртуальные частные сети (VPN). Назначение, основные возможности, принципы функционирования и варианты реализации. Структура защищенной корпоративной сети. Варианты, достоинства и недостатки VPN-решений. Общие рекомендации по их применению (1 час).;
12. 1.Основные понятия безопасности электронного бизнеса. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информационных систем (1 час).;
13. 7.Определение требований к защищенности ресурсов. Обследование подсистем, инвентаризация и категорирование ресурсов информационных систем. Положение о категорировании ресурсов. Перечень информационных ресурсов, подлежащих защите (1 час).;
14. 16.Средства выявления уязвимостей узлов сетей и средства обнаружения атак на узлы, протоколы и сетевые службы. Назначение, возможности, принципы работы. Сравнение возможностей с межсетевыми экранами. Варианты решений по обеспечению безопасности сети организации (1 час).;
15. 6.Обеспечение безопасности в банковской сфере. Электронные платежные системы. Классификация и особенности применения в РФ. Основные принципы внедрения платежных систем в электронную коммерцию. Система организационно-распорядительных документов организации по вопросам обеспечения безопасности информационных технологий. Регламентация действий всех категорий сотрудников, допущенных к работе с информационными системами (1 час).;
16. 14.Контроль информационного наполнения (контента) электронной почты и Web-трафика. Компоненты и функционирование систем контроля контента. Политики безопасности, сценарии и варианты применения и реагирования (1 час)..

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основные модели электронной коммерции"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Угрозы безопасности электронной коммерции и электронных платежей. Безопасность банковских структур"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методы и средства обеспечения информационной безопасности электронного бизнеса"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Политика информационной безопасности. Построение систем безопасности электронного бизнеса"

3.6 Тематика курсовых проектов/курсовых работ
Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)				Оценочное средство (тип и наименование)
		1	2	3	4	
Знать:						
методы защиты конфиденциальной информации (правовые, организационные, программные и аппаратные) при организации и поддержке электронного бизнеса	ПК-3(Компетенция)	+				Контрольная работа/Контрольная работа №1 : Структура основных бизнес-моделей элек-тронной коммерции. Основные отличия и особенности моделей. Обзор со-временных форм и методов ведения ЭБ в РФ. Выбор вида ЭБ для своего варианта предприятия
Уметь:						
администрировать подсистемы информационной безопасности объекта защиты	ПК-3(Компетенция)				+	Контрольная работа/Контрольная работа №3 : Расчет величины стоимости ущерба и вероятности атаки. Расчет стоимости ущерба от атак на предприятие электронного бизнеса. Расчет рисков потери информации на предприятии (вариант)
применять навыки в области применения защитных механизмов при организации и ведении электронного бизнеса	ПК-13(Компетенция)		+	+		Контрольная работа/Контрольная работа №4 : Выбор угроз для своего выбранного пред-приятия электронного бизнеса. Построение схемы угроз. Перечень угроз. Выстраивание модели злоумышленника на своем предприятии
организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности организации	ПК-13(Компетенция)			+		Контрольная работа/Контрольная работа №2 Правовое регулирование отношений в сфере защиты информации Российское законодательство в сфере обеспечения информационной безопасности. Алгоритм построения систем защиты ЭБ. Контрольная работа/Контрольная работа №4 : Выбор угроз для своего выбранного пред-приятия электронного бизнеса. Построение схемы угроз. Перечень угроз. Выстраивание модели злоумышленника на своем

						предприятии

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

8 семестр

Форма реализации: Письменная работа

1. Контрольная работа №1 : Структура основных бизнес-моделей элек-тронной коммерции. Основные отличия и особенности моделей. Обзор со-временных форм и методов ведения ЭБ в РФ. Выбор вида ЭБ для своего варианта предприятия (Контрольная работа)
2. Контрольная работа №2 Правовое регулирование отношений в сфере защиты информации Российское законодательство в сфере обеспечения информационной безопасности. Алгоритм построения систем защиты ЭБ. (Контрольная работа)
3. Контрольная работа №3 : Расчет величины стоимости ущерба и вероятности атаки. Расчет стоимости ущерба от атак на предприятие электронного бизнеса. Расчет рисков потери информации на предприятии (вариант) (Контрольная работа)
4. Контрольная работа №4 : Выбор угроз для своего выбранного пред-приятия электронного бизнеса. Построение схемы угроз. Перечень угроз. Выстраивание модели злоумышленника на своем предприятии (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании экзаменационной составляющей.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Лапидус, Л. В. Цифровая экономика. Управление электронным бизнесом и электронной коммерцией : учебник для вузов по направлениям 38.03.01 "Экономика", 38.03.02 "Менеджмент" (квалификация (степень) "бакалавр") / Л. В. Лапидус, Моск. гос. ун-т им. М.В. Ломоносова (МГУ) . – Москва : ИНФРА-М, 2020 . – 479 с. – (Высшее образование . Бакалавриат) . - ISBN 978-5-16-013640-0 .;
2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие по направлению "Прикладная информатика" / Е. К. Баранова, А. В. Бабаш . – 3-е изд., перераб. и доп . – М. : РИОР : ИНФРА-М, 2017 . – 322 с. – (Высшее образование) . - ISBN 978-5-369-01450-9 .;
3. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие для среднего профессионального образования / А. В. Васильков, И. А. Васильков . – М. : Форум : ИНФРА-М, 2018 . – 368 с. – (Среднее профессиональное образование) . - ISBN 978-5-91134-360-6 .;
4. Г. И. Курчеева, М. А. Бакаев, В. А. Хворостов- "Информационное и программное обеспечение электронного бизнеса", Издательство: "Новосибирский государственный

технический университет", Новосибирск, 2018 - (107 с.)
https://biblioclub.ru/index.php?page=book&id=576386;
5. Сковиков А. Г.- "Цифровая экономика. Электронный бизнес и электронная коммерция", (2-е изд., стер.), Издательство: "Лань", Санкт-Петербург, 2021 - (260 с.)
https://e.lanbook.com/book/152653;
6. Д. П. Денисов- "Интернет-технологии в электронном бизнесе и коммерции", Издательство: "Лаборатория книги", Москва, 2012 - (112 с.)
https://biblioclub.ru/index.php?page=book&id=140249.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office;
3. Windows;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Scopus** - http://www.scopus.com
6. **Национальная электронная библиотека** - https://rusneb.ru/
7. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
8. **Журнал Science** - https://www.sciencemag.org/
9. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
10. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
11. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в

		Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечение безопасности электронного бизнеса

(название дисциплины)

8 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 Контрольная работа №1 : Структура основных бизнес-моделей элек-тронной коммерции. Основные отличия и особенности моделей. Обзор со-временных форм и методов ведения ЭБ в РФ. Выбор вида ЭБ для своего варианта предприятия (Контрольная работа)

КМ-2 Контрольная работа №2 Правовое регулирование отношений в сфере защиты информации Российское законодательство в сфере обеспечения информационной безопасности. Алгоритм построения систем защиты ЭБ. (Контрольная работа)

КМ-3 Контрольная работа №3 : Расчет величины стоимости ущерба и вероятности атаки. Расчет стоимости ущерба от атак на предприятие электронного бизнеса. Расчет рисков потери информации на предприятии (вариант) (Контрольная работа)

КМ-4 Контрольная работа №4 : Выбор угроз для своего выбранного пред-приятия электронного бизнеса. Построение схемы угроз. Перечень угроз. Выстраивание модели злоумышленника на своем предприятии (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	16
1	Основные модели электронной коммерции					
1.1	Тема 1. Введение в дисциплину		+			
2	Угрозы безопасности электронной коммерции и электронных платежей. Безопасность банковских структур					
2.1	Потенциальные угрозы электронного бизнеса					+
2.2	Построение модели злоумышленника					+
2.3	Классификация преступлений в электронном бизнесе					+
3	Методы и средства обеспечения информационной безопасности электронного бизнеса					
3.1	Правовые основы обеспечения информационной безопасности			+		+
3.2	Методы контроля и разграничения доступа к информации			+		+
3.3	Использование механизмов и средств криптографической защиты информации в системах электронного бизнеса			+		+
3.4	Основы безопасности электронной торговли при использовании пластиковых карт. К			+		+

4	Политика информационной безопасности. Построение систем безопасности электронного бизнеса				
4.1	Политика информационной безопасности в системах электронной коммерции			+	
4.2	Стандарт Центрального банка России по защите информации (СТО БР ИББС-1.0–2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (с изменениями 2010 и 2014 г.)			+	
4.3	Основы построения и менеджмента систем безопасности электронного бизнеса. Аудит систем информационной безопасности электронного бизнеса			+	
	Вес КМ, %:	25	25	25	25